SECTION 28 13 00
PHYSICAL ACCESS CONTROL SYSTEM

SPEC WRITER NOTE: Delete // _____ // if not applicable to project. Also delete any other item or paragraph not applicable in the section and renumber the paragraphs. Insert additional provisions as required for this project.

PART 1 – GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operating Physical Access Control System, hereinafter referred to as the PACS.

B. This Section includes a Physical Access Control System consisting of a system server, [one or more networked workstation computers,] operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The PACS shall have the following:

SPEC WRITER NOTE: Adjust list to suit the project.

1. Physical Access Control:
   a. Regulating access through doors [, gates] [, traffic-control bollards] <List other access-control devices>
   b. Anti-passback
   c. Visitor assignment
   d. Surge and tamper protection
   e. Secondary alarm annunciator
   f. Credential cards and readers
   g. Biometric identity verification equipment
   h. Push-button switches
   i. RS-232 ASCII interface
   j. Credential creation and credential holder database and management
   k. Monitoring of field-installed devices
   l. Interface with [paging] [HVAC] [elevator control] <Insert other> systems.
   m. Reporting

SPEC WRITER NOTE: Edit list of security functions below to be integrated into or coordinated with access-control system. Items listed above are described in this Section; items listed below are traditionally specified in other Sections. If items below are specified

in other Sections, special coordination is required in those Sections. For example, "Key Tracking" software in this Section is more comprehensive than manual tracking specified in Division 08 Sections.

2. Security:
   a. Real-time guard tour.
   b. Time and attendance.
   c. Key tracking.
   d. Video and camera control.
   e. Time and attendance
   f. <Insert name of system.>

C. System Architecture:
   1. Criticality, operational requirements, and/or limiting points of failure may dictate the development of an enterprise and regional server architecture as opposed to system capacity. Provide server and workstation configurations with all necessary connectors, interfaces and accessories as shown.

D. PACS shall provide secure and reliable identification of Federal employees and contractors by utilizing credential authentication per FIPS-201.

E. Physical Access Control System (PACS) shall consist of:
   1. Head-End equipment server,
   2. One or more networked PC-based workstations,
   3. Physical Access Control System and Database Management Software,
   4. Credential validation software/hardware,
   5. Field installed controllers,
   6. PIV Middelware,
   7. Card readers,
   8. Biometric identification devices,
   9. PIV <PIV-I>, <Legacy CAC>, <CAC NG>, <CAC EP>, <TWIC>, <FRAC> cards,
   10. Supportive information system,
   11. Door locks and sensors,
   12. Power supplies,
   13. Interfaces with:
      a. Video Surveillance and Assessment System,
      b. Gate, turnstile, and traffic arm controls,
      c. Automatic door operators,
      d. Intrusion Detection System,

e. Intercommunication System
f. Fire Protection System,
g. HVAC,
h. Building Management System,
i. Elevator Controls,
j. <list interfaced systems>.

14. <list system components>.

F. Head-End equipment server, workstations and controllers shall be connected by a high-speed electronic data transmission network.

G. Information system supporting PACS , Head-End equipment server, workstations, network switches, routers and controllers shall comply with FIPS 200 requirements (Minimum Security Requirements for Federal Information and Information Systems)and NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).

H. PACS system shall support:
1. Multiple credential authentication modes,
2. Bidirectional communication with the reader,
3. Incident response policy implementation capability; system shall have capability to automatically change access privileges for certain user groups to high security areas in case of incident/emergency.
4. Visitor management,

I. All security relevant decisions shall be made on “secure side of the door”. Secure side processing shall include;
1. Challenge/response management,
2. PKI path discovery and validation,
3. Credential identifier processing,
4. Authorization decisions.

J. For locations where secure side processing is not applicable the tamper switches and certified cryptographic processing shall be provided per FIPS-140-2.

K. System Software: Based on <Insert name of operating system> central-station, workstation operating system, server operating system, and application software.

L. Software and controllers shall be capable of matching full 56 bit FASC-N plus minimum of 32 bits of public key certificate data.

M. Software shall have the following capabilities:

1. Multiuser multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Support authentication and enrolment;
   a. PIV verification,
   b. Expiration date check,
   c. Biometric check,
   d. Digital photo display/check,
   e. Validate digital signatures of data objects (Objects are signed by the Trusted Authority
   f. Private key challenge (CAK & PAK to verify private key public key pairs exist and card is not a clone)
3. Support CRL validation via OCSP or SCVP on a scheduled basis and automatically deny access to any revoked credential in the system.
4. Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
5. System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section.
6. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with <insert operating system> operating system.
7. Operator login and access shall be utilized via integrated smart card reader and password protection.

N. Systems Networks:
   1. A standalone system network shall interconnect all components of the system. This network shall include communications between a central station and any peer or subordinate workstations, enrollment stations, local annunciation stations, portal control stations or redundant central stations.

SPEC WRITER NOTE: Edit paragraph O. per project requirements.

O. Security Management System Server Redundancy:
   1. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:
      a. Hot Standby Servers
      b. Clustering
      c. Disk Mirroring
      d. RAID Level 10

e. Distributed Intelligence

P. Number of points:

1. PACS shall support multiple autonomous regional servers that can connect to a master command and controller server.
2. Unlimited number of access control readers, unlimited number of inputs or outputs, unlimited number of client workstations, unlimited number of cardholders.
3. Total system solution to enable enterprise-wide, networked, multi-user access to all system resources via a wide range of options for connectivity with the customer’s existing LAN and WAN.

Q. Console Network:

1. Console network, if required, shall provide communication between a central station and any subordinate or separate stations of the system. Where redundant central or parallel stations are required, the console network shall allow the configuration of stations as master and slave. The console network may be a part of the field device network or may be separate depending upon the manufacturer's system configuration.

R. Network(s) connecting PCs and Controllers shall comply with NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) and consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet [10 BASE-T] [100 BASE-TX], star topology network based on TCP/IP.
2. Direct-connected, RS-232 cable from the COM port of the Central Station to the first Controller, then RS-485 to interconnect the remainder of the Controllers at that Location.

1.2 RELATED WORK

SPEC WRITER NOTE: Delete any item or paragraph not applicable in the section and renumber the paragraphs.

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 08 11 73 - SLIDING METAL FIRE DOORS. Requirements for door installation.

D. Section 08 34 59 - VAULT DOORS AND DAY GATES. Requirements for door and gate installation.

E. Section 08 35 13.13 - ACCORDIAN FOLDING DOORS. Requirements for door installation.
F. Section 08 71 00 - DOOR HARDWARE. Requirements for door installation.
G. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.
H. Section 14 21 00 ELECTRIC TRACTION ELEVATORS. Requirements for elevators.
I. Section 14 24 00 - HYDRAULIC ELEVATORS. Requirements for elevators.
J. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.
K. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.
L. Section 26 05 33 – RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.
M. Section 26 05 41 - UNDERGROUND ELECTRICAL CONSTRUCTION. Requirements for underground installation of wiring.
N. Section 26 56 00 - EXTERIOR LIGHTING. Requirements for perimeter lighting.
O. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.
P. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
Q. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.
R. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.
S. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY. For requirements for commissioning, systems readiness checklists, and training.
T. Section 28 13 16 - ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT. Requirements for control and operation of all security systems.
U. Section 28 13 53 - SECURITY ACCESS DETECTION. Requirements for screening of personnel and shipments.
V. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.
W. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

X. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

Y. Section 28 31 00 - FIRE DETECTION AND ALARM. Requirements for integration with fire detection and alarm system.

1.3 QUALITY ASSURANCE

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. The Contractor shall be responsible for providing, installing, and the operation of the PACS as shown. The Contractor shall also provide certification as required.

B. The security system will be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the security system is stand-alone or a part of a complete Information Technology (IT) computer network.

C. Manufacturers Qualifications: The manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, the equipment and material specified for this project, and shall have manufactured the item for at least three years.

D. Product Qualifications:

1. Manufacturer's product shall have been in satisfactory operation, on three installations of similar size and type as this project, for approximately three years.
2. The Government reserves the right to require the Contractor to submit a list of installations where the products have been in operation before approval.

E. Contractor Qualifications:

1. The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years experience installing and servicing systems of similar scope and complexity. The Contractor shall be an authorized regional representative of the Security Management System’s (PACS) manufacturer. The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity which became operational in the past three (3) years. At least three (3) of the references shall be utilizing the same system components, in a similar configuration as the proposed system. The references must include a current point of contact, company or agency name, address, telephone number, complete

system description, date of completion, and approximate cost of the project. The owner reserves the option to visit the reference sites, with the site owner's permission and representative, to verify the quality of installation and the references' level of satisfaction with the system. The Contractor shall provide copies of system manufacturer certification for all technicians. The Contractor shall only utilize factory-trained technicians to install, program, and service the PACS. The Contractor shall only utilize factory-trained technicians to install, terminate and service controller/field panels and reader modules. The technicians shall have a minimum of five (5) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within 60 miles of the project site. The local facility shall include sufficient spare parts inventory to support the service requirements associated with this contract. The facility shall also include appropriate diagnostic equipment to perform diagnostic procedures. The Resident Engineer reserves the option of surveying the company's facility to verify the service inventory and presence of a local service organization.

a. The Contractor shall provide proof project superintendent with BICSI Certified Commercial Installer Level 1, Level 2, or Technician to provide oversight of the project.
b. Cable installer must have on staff a Registered Communication Distribution Designer (RCDD) certified by Building Industry Consulting Service International. The staff member shall provide consistent oversight of the project cabling throughout design, layout, installation, termination and testing.

SPEC WRITER NOTE: In the following paragraph use 4 hours for metropolitan areas and 8 hours for rural areas.

F. Service Qualifications: There shall be a permanent service organization maintained or trained by the manufacturer which will render satisfactory service to this installation within // four // eight // hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.4 SUBMITTALS

SPEC WRITER NOTE: Delete and/or amend all paragraphs and sub-paragraphs and information as needed to ensure that only

the documentation required is requested per the Request for Proposal (RFP).

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, Section 02 41 00, DEMOLITION, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

B. Provide certificates of compliance with Section 1.3, Quality Assurance.

C. Provide a complete and thorough pre-installation and as-built design package in both electronic format and on paper, minimum size 48 x 48 inches (1220 x 1220 millimeters); drawing submittals shall be per the established project schedule.

D. Shop drawing and as-built packages shall include, but not be limited to:

1. Index Sheet that shall:
   a. Define each page of the design package to include facility name, building name, floor, and sheet number.
   b. Provide a complete list of all security abbreviations and symbols.
   c. Reference all general notes that are utilized within the design package.
   d. Specification and scope of work pages for all individual security systems that are applicable to the design package that will:
      1) Outline all general and job specific work required within the design package.
      2) Provide a detailed device identification table outlining device Identification (ID) and use for all security systems equipment utilized in the design package.
2. Drawing sheets that will be plotted on the individual floor plans or site plans shall:
   a. Include a title block as defined above.
   b. Clearly define the drawings scale in both standard and metric measurements.
   c. Provide device identification and location.
   d. Address all signal and power conduit runs and sizes that are associated with the design of the electronic security system and other security elements (e.g., barriers, etc.).

e. Identify all pull box and conduit locations, sizes, and fill capacities.
f. Address all general and drawing specific notes for a particular drawing sheet.

3. A detailed riser drawing for each applicable security subsystem shall:
   a. Indicate the sequence of operation.
   b. Relationship of integrated components on one diagram.
   c. Include the number, size, identification, and maximum lengths of interconnecting wires.
   d. Wire/cable types shall be defined by a wire and cable schedule. The schedule shall utilize a lettering system that will correspond to the wire/cable it represents (example: A = 18 AWG/1 Pair Twisted, Unshielded). This schedule shall also provide the manufacturer’s name and part number for the wire/cable being installed.
4. A detailed system drawing for each applicable security system shall:
   a. Clearly identify how all equipment within the system, from main panel to device, shall be laid out and connected.
   b. Provide full detail of all system components wiring from point-to-point.
   c. Identify wire types utilized for connection, interconnection with associate security subsystems.
   d. Show device locations that correspond to the floor plans.
   e. All general and drawing specific notes shall be included with the system drawings.
5. A detailed schedule for all of the applicable security subsystems shall be included. All schedules shall provide the following information:
   a. Device ID.
   b. Device Location (e.g. site, building, floor, room number, location, and description).
   c. Mounting type (e.g. flush, wall, surface, etc.).
   d. Power supply or circuit breaker and power panel number.
   e. In addition, for the PACS, provide the door ID, door type (e.g. wood or metal), locking mechanism (e.g. strike or electromagnetic lock) and control device (e.g. card reader or biometrics).

6. Detail and elevation drawings for all devices that define how they were installed and mounted.

E. Pre-installation design packages shall go through a full review process conducted by the Contractor along with a VA representative to ensure all work has been clearly defined and completed. All reviews shall be conducted in accordance with the project schedule. There shall be four (4) stages to the review process:
   1. 35 percent
   2. 65 percent
   3. 90 percent
   4. 100 percent

F. Provide manufacturer security system product cut-sheets. Submit for approval at least 30 days prior to commencement of formal testing, a Security System Operational Test Plan. Include procedures for operational testing of each component and security subsystem, to include performance of an integrated system test.

G. Submit manufacture’s certification of Underwriters Laboratories, Inc. (UL) listing as specified. Provide all maintenance and operating manuals per Section 01 00 00, GENERAL REQUIREMENTS, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

H. Completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

I. General: Submittals shall be in full compliance of the Contract Documents. All submittals shall be provided in accordance with this section. Submittals lacking the breath or depth these requirements will be considered incomplete and rejected. Submissions are considered multidisciplinary and shall require coordination with applicable divisions to provide a complete and comprehensive submission package. Additional general provisions are as follows:
   1. The Contractor shall schedule submittals in order to maintain the project schedule. For coordination drawings refer to Specification Section 01 33 10 - DESIGN SUBMITTAL PROCEDURES, which outline basic submittal requirements and coordination. Section 01 33 10 shall be used in conjunction with this section.

2. The Contractor shall identify variations from requirements of Contract Documents and state product and system limitations, which may be detrimental to successful performance of the completed work or system.
3. Each package shall be submitted at one (1) time for each review and include components from applicable disciplines (e.g., electrical work, architectural finishes, door hardware, etc.) which are required to produce an accurate and detailed depiction of the project.
4. Manufacturer’s information used for submittal shall have pages with items for approval tagged, items on pages shall be identified, and capacities and performance parameters for review shall be clearly marked through use of an arrow or highlighting. Provide space for Resident Engineer and Contractor review stamps.
5. Technical Data Drawings shall be in the latest version of AutoCAD®, drawn accurately, and in accordance with VA CAD Standards. FREEHAND SKETCHES OR COPIED VERSIONS OF THE CONSTRUCTION DOCUMENTS WILL NOT BE ACCEPTED. The Contractor shall not reproduce Contract Documents or copy standard information as the basis of the Technical Data Drawings. If departures from the technical data drawings are subsequently deemed necessary by the Contractor, details of such departures and the reasons thereof shall be submitted in writing to the Resident Engineer for approval before the initiation of work.
6. Packaging: The Contractor shall organize the submissions according to the following packaging requirements.
   a. Binders: For each manual, provide heavy duty, commercial quality, durable three (3) ring vinyl covered loose leaf binders, sized to receive 8.5 x 11 in paper, and appropriate capacity to accommodate the contents. Provide a clear plastic sleeve on the spine to hold labels describing the contents. Provide pockets in the covers to receive folded sheets.
      1) Where two (2) or more binders are necessary to accommodate data, correlate data in each binder into related groupings according to the Project Manual table of contents. Cross-referencing other binders where necessary to provide essential information for communication of proper operation and or maintenance of the component or system.

2) Identify each binder on the front and spine with printed binder title, Project title or name, and subject matter covered. Indicate the volume number if applicable.

b. Dividers: Provide heavy paper dividers with celluloid tabs for each Section. Mark each tab to indicate contents.

c. Protective Plastic Jackets: Provide protective transparent plastic jackets designed to enclose diagnostic software for computerized electronic equipment.

d. Text Material: Where written material is required as part of the manual use the manufacturer's standard printed material, or if not available, specially prepared data, neatly typewritten on 8.5 inches by 11 inches 20 pound white bond paper.

e. Drawings: Where drawings and/or diagrams are required as part of the manual, provide reinforced punched binder tabs on the drawings and bind them with the text.

1) Where oversized drawings are necessary, fold the drawings to the same size as the text pages and use as a foldout.

2) If drawings are too large to be used practically as a foldout, place the drawing, neatly folded, in the front or rear pocket of the binder. Insert a type written page indicating the drawing title, description of contents and drawing location at the appropriate location of the manual.

3) Drawings shall be sized to ensure details and text is of legible size. Text shall be no less than 1/16” tall.

f. Manual Content: In each manual include information specified in the individual Specification section, and the following information for each major component of building equipment and controls:

1) General system or equipment description.

2) Design factors and assumptions.

3) Copies of applicable Shop Drawings and Product Data.

4) System or equipment identification including: manufacturer, model and serial numbers of each component, operating instructions, emergency instructions, wiring diagrams, inspection and test procedures, maintenance procedures and schedules, precautions against improper use and maintenance, repair instructions, sources of required maintenance materials and related services, and a manual index.

g. Binder Organization: Organize each manual into separate sections for each piece of related equipment. At a minimum, each manual shall contain a title page, table of contents, copies of Product Data supplemented by drawings and written text, and copies of each warranty, bond, certifications, and service Contract issued. Refer to Group I through V Technical Data Package Submittal requirements for required section content.
h. Title Page: Provide a title page as the first sheet of each manual to include the following information; project name and address, subject matter covered by the manual, name and address of the Project, date of the submittal, name, address, and telephone number of the Contractor, and cross references to related systems in other operating and/or maintenance manuals.
i. Table of Contents: After the title page, include a type written table of contents for each volume, arranged systematically according to the Project Manual format. Provide a list of each product included, identified by product name or other appropriate identifying symbols and indexed to the content of the volume. Where more than one (1) volume is required to hold data for a particular system, provide a comprehensive table of contents for all volumes in each volume of the set.
j. General Information Section: Provide a general information section immediately following the table of contents, listing each product included in the manual, identified by product name. Under each product, list the name, address, and telephone number of the installer and maintenance Contractor. In addition, list a local source for replacement parts and equipment.
k. Drawings: Provide specially prepared drawings where necessary to supplement the manufacturers printed data to illustrate the relationship between components of equipment or systems, or provide control or flow diagrams. Coordinate these drawings with information contained in Project Record Drawings to assure correct illustration of the completed installation.
l. Manufacturer’s Data: Where manufacturer's standard printed data is included in the manuals, include only those sheets that are pertinent to the part or product installed. Mark each sheet to identify each part or product included in the installation. Where more than one (1) item in tabular format is included,

identify each item, using appropriate references from the Contract Documents. Identify data that is applicable to the installation and delete references to information which is not applicable.

m. Where manufacturer's standard printed data is not available and the information is necessary for proper operation and maintenance of equipment or systems, or it is necessary to provide additional information to supplement the data included in the manual, prepare written text to provide the necessary information. Organize the text in a consistent format under a separate heading for different procedures. Where necessary, provide a logical sequence of instruction for each operating or maintenance procedure. Where similar or more than one product is listed on the submittal the Contractor shall differentiate by highlighting the specific product to be utilized.

n. Calculations: Provide a section for circuit and panel calculations.

o. Loading Sheets: Provide a section for DGP Loading Sheets.

p. Certifications: Provide section for Contractor’s manufacturer certifications.

7. Contractor Review: Review submittals prior to transmittal. Determine and verify field measurements and field construction criteria. Verify manufacturer’s catalog numbers and conformance of submittal with requirements of contract documents. Return non-conforming or incomplete submittals with requirements of the work and contract documents. Apply Contractor’s stamp with signature certifying the review and verification of products occurred, and the field dimensions, adjacent construction, and coordination of information is in accordance with the requirements of the contract documents.
8. Resubmission: Revise and resubmit submittals as required within 15 calendar days of return of submittal. Make resubmissions under procedures specified for initial submittals. Identify all changes made since previous submittal.
9. Product Data: Within 15 calendar days after execution of the contract, the Contractor shall submit for approval a complete list of all of major products proposed for use. The data shall include name of manufacturer, trade name, model number, the associated

contract document section number, paragraph number, and the referenced standards for each listed product.

J. Group 1 Technical Data Package: Group I Technical Data Package shall be one submittal consisting of the following content and organization. Refer to VA Special Conditions Document for drawing format and content requirements. The data package shall include the following:

1. Section I - Drawings:
   a. General – Drawings shall conform to VA Special Conditions and CAD Standards Documents. All text associated with security details shall be 1/8″ tall and meet VA text standard for AutoCAD™ drawings.
   b. Cover Sheet – Cover sheet shall consist of Project Title and Address, Project Number, Area and Vicinity Maps.
   c. General Information Sheets – General Information Sheets shall consist of General Notes, Abbreviations, Symbols, Wire and Cable Schedule, Project Phasing, and Sheet Index.
   d. Floor Plans – Floor plans shall be produced from the Architectural backgrounds issued in the Construction Documents. The contractor shall receive floor plans from the prime A/E to develop these drawing sets. Security devices shall be placed on drawings in scale. All text associated with security details shall be 1/8″ tall and meet VA text standard for AutoCAD™ drawings. Floor plans shall identify the following:
      1) security devices by symbol,
      2) the associated device point number (derived from the loading sheets),
      3) wire & cable types and counts
      4) conduit sizing and routing
      5) conduit riser systems
      6) device and area detail call outs
   e. Architectural details – Architectural details shall be produced for each device mounting type (door details for doors with physical access control, reader pedestals and mounts, security panel and power supply details).
   f. Riser Diagrams – Contractor shall provide a riser diagram indicating riser architecture and distribution of the physical access control system throughout the facility (or area in scope).

g. Block Diagrams – Contractor shall provide a block diagram for the entire system architecture and interconnections with SMS subsystems. Block diagram shall identify SMS subsystem (e.g., physical access control, intrusion detection, closed circuit television, intercom, and other associated subsystems) integration; and data transmission and media conversion methodologies.
h. Interconnection Diagrams – Contractor shall provide interconnection diagram for each sensor, and device component. Interconnection diagram shall identify termination locations, standard wire detail to include termination schedule. Diagram shall also identify interfaces to other systems such as elevator control, fire alarm systems, and security management systems.
i. Security Details:
    1) Panel Assembly Detail – For each panel assembly, a panel assembly details shall be provided identifying individual panel component size and content.
    2) Panel Details – Provide security panel details identify general arrangement of the security system components, backboard size, wire through size and location, and power circuit requirements.
    3) Device Mounting Details – Provide mounting detailed drawing for each security device (physical access control system, intrusion detection, video surveillance and assessment, and intercom systems) for each type of wall and ceiling configuration in project. Device details shall include device, mounting detail, wiring and conduit routing.
    4) Details of connections to power supplies and grounding
    5) Details of surge protection device installation
    6) Sensor detection patterns – Each system sensor shall have associated detection patterns.
    7) Equipment Rack Detail – For each equipment rack, provide a scaled detail of the equipment rack location and rack space utilization. Use of BISCI wire management standards shall be employed to identify wire management methodology. Transitions between equipment racks shall be shown to include use vertical and horizontal latter rack system.

8) Security Control Room – The contractor shall provide a layout plan for the Security Control Room. The layout plan shall identify all equipment and details associated with the installation.
9) Operator Console – The contractor shall provide a layout plan for the Operator Console. The layout plan shall identify all equipment and details associated with the installation. Equipment room - the contractor shall provide a layout plan for the equipment room. The layout plan shall identify all equipment and details associated with the installation.
10) Equipment Room – Equipment room details shall provide architectural, electrical, mechanical, plumbing, IT/Data and associated equipment and device placements both vertical and horizontally.

j. Electrical Panel Schedule – Electrical Panel Details shall be provided for all SMS systems electrical power circuits. Panel details shall be provided identifying panel type (Standard, Emergency Power, Emergency/Uninterrupted Power Source, and Uninterrupted Power Source Only), panel location, circuit number, and circuit amperage rating.

k. Door Schedule – A door schedule shall be developed for each door equipped with electronic security components. At a minimum, the door schedule shall be coordinated with Division 08 work and include the following information:
1) Item Number
2) Door Number (Derived from A/E Drawings)
3) Floor Plan Sheet Number
4) Standard Detail Number
5) Door Description (Derived from Loading Sheets)
6) Data Gathering Panel Input Number
7) Door Position or Monitoring Device Type & Model Number
8) Lock Type, Model Number & Power Input/Draw (standby/active)
9) Card Reader Type & Model Number
10) Shunting Device Type & Model Number
11) Sounder Type & Model Number
12) Manufacturer
13) Misc. devices as required
a) Delayed Egress Type & Model Number

b) Intercom
c) Camera
d) Electric Transfer Hinge
e) Electric Pass-through device

14) Remarks column indicating special notes or door configurations

2. Camera Schedule - A camera schedule shall be developed for each camera. Contractors shall coordinate with the Resident Engineer to determine camera starting numbers and naming conventions. All drawings shall identify wire and cable standardization methodology. Color coding of all wiring conductors and jackets is required and shall be communicated consistently throughout the drawings package submittal. At a minimum, the camera schedule shall include the following information:
   a. Item Number
   b. Camera Number
   c. Naming Conventions
   d. Description of Camera Coverage
   e. Camera Location
   f. Floor Plan Sheet Number
   g. Camera Type
   h. Mounting Type
   i. Standard Detail Reference
   j. Power Input & Draw
   k. Power Panel Location
   l. Remarks Column for Camera
3. Section II – Data Gathering Panel Documentation Package
   a. Contractor shall provide Data Gathering Panel (DGP) input and output documentation packages for review at the Shop Drawing submittal stage and also with the as-built documentation package. The documentation packages shall be provided in both printed and magnetic form at both review stages.
   b. The Contractor shall provide loading sheet documentation package for the associated DGP, including input and output boards for all field panels associated with the project. Documentation shall be provided in current version Microsoft Excel spreadsheets following the format currently utilized by VA. A separate spreadsheet file shall be generated for each DGP and associated field panels.

c. The spreadsheet names shall follow a sequence that shall display the spreadsheets in numerical order according to the DGP system number. The spreadsheet shall include the prefix in the file name that uniquely identifies the project site. The spreadsheet shall detail all connected items such as card readers, alarm inputs, and relay output connections. The spreadsheet shall include an individual section (row) for each panel input, output and card reader. The spreadsheet shall automatically calculate the system numbers for card readers, inputs, and outputs based upon data entered in initialization fields.
d. All entries must be verified against the field devices. Copies of the floor plans shall be forwarded under separate cover.
e. The DGP spreadsheet shall include an entry section for the following information:
   1) DGP number
   2) First Reader Number
   3) First Monitor Point Number
   4) First Relay Number
   5) DGP, input or output Location
   6) DGP Chain Number
   7) DGP Cabinet Tamper Input Number
   8) DGP Power Fail Input Number
   9) Number of Monitor Points Reserved For Expansion Boards
   10) Number of Control Points (Relays) Reserved For Expansion Boards
f. The DGP, input module and output module spreadsheets shall automatically calculate the following information based upon the associated entries in the above fields:
   1) System Numbers for Card Readers
   2) System Numbers for Monitor Point Inputs
   3) System Numbers for Control Points (Relays)
   4) Next DGP or input module First Monitor Point Number
   5) Next DGP or output module First Control Point Number
g. The DGP spreadsheet shall provide the following information for each card reader:
   1) DGP Reader Number
   2) System Reader Number
   3) Cable ID Number

4) Description Field (Room Number)
5) Description Field (Device Type i.e.: In Reader, Out Reader, etc.)
6) Description Field
7) DGP Input Location
8) Date Test
9) Date Passed
10) Cable Type
11) Camera Numbers (of cameras viewing the reader location)

h. The DGP and input module spreadsheet shall provide the following information for each monitor point (alarm input).
1) DGP Monitor Point Input Number
2) System Monitor Point Number
3) Cable ID Number
4) Description Field (Room Number)
5) Description Field (Device Type i.e.: Door Contact, Motion Detector, etc.)
6) DGP or input module Input Location
7) Date Test
8) Date Passed
9) Cable Type
10) Camera Numbers (of associated alarm event preset call-ups)

i. The DGP and output module spreadsheet shall provide the following information for each control point (output relay).
1) DGP Control Point (Relay) Number
2) System (Control Point) Number
3) Cable ID Number
4) Description Field (Room Number)
5) Description Field (Device: Lock Control, Local Sounder, etc.)
6) Description Field
7) DGP or OUTPUT MODULE Output Location
8) Date Test
9) Date Passed Cable Type
10) Camera Number (of associated alarm event preset call-ups)

j. The DGP, input module and output module spreadsheet shall include the following information or directions in the header and footer:
1) Header
a) DGP Input and Output Worksheet

b) Enter Beginning Reader, Input, and Output Starting Numbers and Sheet Will Automatically Calculate the Remaining System Numbers.

2) Footer

a) File Name

b) Date Printed

c) Page Number

SPEC WRITER NOTE: Delete following paragraph describing Mock-up construction if not required by the project.

4. Section III - Construction Mock-up: In areas with exposed EMT/Conduit Raceways, contractor shall conceal raceway as much as practical and unobtrusively. In addition, historic significance must be considered to determine installation means and methods for approval by the owner.
5. Section IV - Manufacturers' Data: The data package shall include manufacturers' data for all materials and equipment, including sensors, local processors and console equipment provided under this specification.
6. Section V - System Description and Analysis: The data package shall include system descriptions, analysis, and calculations used in sizing equipment required by these specifications. Descriptions and calculations shall show how the equipment will operate as a system to meet the performance requirements of this specification. The data package shall include the following:
   a. Central processor memory size; communication speed and protocol description; rigid disk system size and configuration; flexible disk system size and configuration; back-up media size and configuration; alarm response time calculations; command response time calculations; start-up operations; expansion capability and method of implementation; sample copy of each report specified; and color photographs representative of typical graphics.
   b. Software Data: The data package shall consist of descriptions of the operation and capability of the system, and application software as specified.
   c. Overall System Reliability Calculations: The data package shall include all manufacturers' reliability data and calculations required to show compliance with the specified reliability.

7. Section VI – Certifications & References: All specified manufacturer’s certifications shall be included with the data package. Contractor shall provide Project references as outlined in Paragraph 1.4 “Quality Assurance”.

K. Group II Technical Data Package
   1. The Contractor shall prepare a report of “Current Site Conditions” and submit a report to the Resident Engineer documenting changes to the site, particularly those conditions that affect performance of the system to be installed. The Contractor shall provide specification sheets, or written functional requirements to support the findings, and a cost estimate to correct those site changes or conditions which affect the installation of the system or its performance. The Contractor shall not correct any deficiency without written permission from the COTR.
   2. System Configuration and Functionality: The contractor shall provide the results of the meeting with VA to develop system requirements and functionality including but not limited to:
      a. Baseline configuration
      b. Access levels
      c. Schedules (intrusion detection, physical access control, holidays, etc.)
      d. Badge database
      e. System monitoring and reporting (unit level and central control)
      f. Naming conventions and descriptors

L. Group III Technical Data Package
   1. Development of Test Procedures: The Contractor will prepare performance test procedures for the system testing. The test procedures shall follow the format of the VA Testing procedures and be customized to the contract requirements. The Contractor will deliver the test procedures to the Resident Engineer for approval at least 60 calendar days prior to the requested test date.

M. Group IV Technical Data Package
   1. Performance Verification Test
      a. Based on the successful completion of the pre-delivery test, the Contractor shall finalize the test procedures and report forms for the performance verification test (PVT) and the endurance test. The PVT shall follow the format, layout and content of the pre-delivery test. The Contractor shall deliver the PVT and

endurance test procedures to the Resident Engineer for approval. The Contractor may schedule the PVT after receiving written approval of the test procedures. The Contractor shall deliver the final PVT and endurance test reports within 14 calendar days from completion of the tests. Refer to Part 3 of this section for System Testing and Acceptance requirements.

2. Training Documentation
   a. New Facilities and Major Renovations: Familiarization training shall be provided for new equipment or systems. Training can include site familiarization training for VA technicians and administrative personnel. Training shall include general information on new system layout including closet locations, turnover of the completed system including all documentation, including manuals, software, key systems, and full system administration rights. Lesson plans and training manuals training shall be oriented to type of training to be provided.
   b. New Unit Control Room:
      1) Provide the security personnel with training in the use, operation, and maintenance of the entire control room system (Unit Control and Equipment Rooms). The training documentation must include the operation and maintenance. The first of the training sessions shall take place prior to system turnover and the second immediately after turnover. Coordinate the training sessions with the Owner. Completed classroom sessions will be witnessed and documented by the Architect/Engineer, and approved by the Resident Engineer. Instruction is not to begin until the system is operational as designed.
      2) The training documents will cover the operation and the maintenance manuals and the control console operators’ manuals and service manuals in detail, stressing all important operational and service diagnostic information necessary for the maintenance and operations personnel to efficiently use and maintain all systems.
      3) Provide an illustrated control console operator's manual and service manual. The operator's manual shall be written in laymen's language and printed so as to become a permanent reference document for the operators, describing all control

panel switch operations, graphic symbol definitions and all indicating functions and a complete explanation of all software.

4) The service manual shall be written in laymen's language and printed so as to become a permanent reference document for maintenance personnel, describing how to run internal self diagnostic software programs, troubleshoot head end hardware and field devices with a complete scenario simulation of all possible system malfunctions and the appropriate corrective measures.

5) Provide a professional color DVD instructional recording of all the operational procedures described in the operator's manual. All charts used in the training session shall be clearly presented on the video. Any DVD found to be inferior in recording or material content shall be reproduced at no cost until an acceptable DVD is submitted. Provide four copies of the training DVD, one to the architect/engineer and three to the owner.

3. System Configuration and Data Entry:

a. The contractor is responsible for providing all system configuration and data entry for the SMS and subsystems (e.g., video matrix switch, intercom, digital video recorders, network video recorders). All data entry shall be performed per VA standards & guidelines. The Contractor is responsible for participating in all meetings with the client to compile the information needed for data entry. These meetings shall be established at the beginning of the project and incorporated in to the project schedule as a milestone task. The contractor shall be responsible for all data collection, data entry, and system configuration. The contractor shall collect, enter, & program and/or configure the following components:

1) Physical Access control system components,

2) All intrusion detection system components,

3) Video surveillance, control and recording systems,

4) Intercom systems components,

5) All other security subsystems shown in the contract documents.

b. The Contractor is responsible for compiling the card access database for the VA employees, including programming reader

configurations, access shifts, schedules, exceptions, card classes and card enrollment databases.

c. Refer to Part 3 for system programming requirements and planning guidelines.

4. Graphics: Based on CAD as-built drawings developed for the construction project, create all map sets showing locations of all alarms and field devices. Graphical maps of all alarm points installed under this contract including perimeter and exterior alarm points shall be delivered with the system. The Contractor shall create and install all graphics needed to make the system operational. The Contractor shall utilize data from the contract documents, Contractor's field surveys, and all other pertinent information in the Contractor's possession to complete the graphics. The Contractor shall identify and request from the COTR, any additional data needed to provide a complete graphics package. Graphics shall have sufficient level of detail for the system operator to assess the alarm. The Contractor shall supply hard copy, color examples at least 203.2 x 254 mm (8 x 10 in) of each type of graphic to be used for the completed Security system. The graphics examples shall be delivered to the Resident Engineer for review and approval at least 90 calendar days prior to the scheduled date the Contractor requires them.

SPEC WRITER NOTE: Edit between //__// as required per Project.

N. Group V Technical Data Package: Final copies of the manuals shall be delivered to the Resident Engineer as part of the acceptance test. The draft copy used during site testing shall be updated with any changes required prior to final delivery of the manuals. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each sub-contractor installing equipment or systems, as well as the nearest service representatives for each item of equipment for each system. The manuals shall include a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include all modifications made during installation, checkout, and acceptance. //Six (6) hard-copies and one (1) soft copy on CD// of each item listed below shall be delivered as a part of final systems acceptance.

1. Functional Design Manual: The functional design manual shall identify the operational requirements for the entire system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes. Manufacturer developed literature may be used; however, shall be produced to match the project requirements.
2. Equipment Manual: A manual describing all equipment furnished including:
   a. General description and specifications; installation and checkout procedures; equipment electrical schematics and layout drawings; system schematics and layout drawings; alignment and calibration procedures; manufacturer’s repair list indicating sources of supply; and interface definition.
3. Software Manual: The software manual shall describe the functions of all software and include all other information necessary to enable proper loading, testing, and operation. The manual shall include:
   a. Definition of terms and functions; use of system and applications software; procedures for system initialization, start-up, and shutdown; alarm reports; reports generation, database format and data entry requirements; directory of all disk files; and description of all communications protocols including data formats, command characters, and a sample of each type of data transfer.
4. Operator’s Manual: The operator’s manual shall fully explain all procedures and instructions for the operation of the system, including:
   a. Computers and peripherals; system start-up and shutdown procedures; use of system, command, and applications software; recovery and restart procedures; graphic alarm presentation; use of report generator and generation of reports; data entry; operator commands’ alarm messages, and printing formats; and system access requirements.
5. Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, recommend schedules, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

6. Spare Parts & Components Data: At the conclusion of the Contractor's work, the Contractor shall submit to the Resident Engineer a complete list of the manufacturer's recommended spare parts and components required to satisfactorily maintain and service the systems, as well as unit pricing for those parts and components.
7. Operation, Maintenance & Service Manuals: The Contractor shall provide two (2) complete sets of operating and maintenance manuals in the form of an instructional manual for use by the VA Security Guard Force personnel. The manuals shall be organized into suitable sets of manageable size. Where possible, assemble instructions for similar equipment into a single binder. If multiple volumes are required, each volume shall be fully indexed and coordinated.
8. Equipment and Systems Maintenance Manual: The Contractor shall provide the following descriptive information for each piece of equipment, operating system, and electronic system:
   a. Equipment and/or system function.
   b. Operating characteristics.
   c. Limiting conditions.
   d. Performance curves.
   e. Engineering data and test.
   f. Complete nomenclature and number of replacement parts.
   g. Provide operating and maintenance instructions including assembly drawings and diagrams required for maintenance and a list of items recommended to stock as spare parts.
   h. Provide information detailing essential maintenance procedures including the following: routine operations, trouble shooting guide, disassembly, repair and re-assembly, alignment, adjusting, and checking.
   i. Provide information on equipment and system operating procedures, including the following; start-up procedures, routine and normal operating instructions, regulation and control procedures, instructions on stopping, shut-down and emergency instructions, required sequences for electric and electronic systems, and special operating instructions.
   j. Manufacturer equipment and systems maintenance manuals are permissible.
9. Project Redlines: During construction, the Contractor shall maintain an up-to-date set of construction redlines detailing

current location and configuration of the project components. The redline documents shall be marked with the words ‘Master Redlines’ on the cover sheet and be maintained by the Contractor in the project office. The Contractor will provide access to redline documents anytime during the project for review and inspection by the Resident Engineer or authorized Office of Protection Services representative. Master redlines shall be neatly maintained throughout the project and secured under lock and key in the contractor’s onsite project office. Any project component or assembly that is not installed in strict accordance with the drawings shall be so noted on the drawings. Prior to producing Record Construction Documents, the contractor will submit the Master Redline document to the Resident Engineer for review and approval of all changes or modifications to the documents. Each sheet shall have Resident Engineer initials indicating authorization to produce “As Built” documents. Field drawings shall be used for data gathering & field changes. These changes shall be made to the master redline documents daily. Field drawings shall not be considered “master redlines”.

10. Record Specifications: The Contractor shall maintain one (1) copy of the Project Specifications, including addenda and modifications issued, for Project Record Documents. The Contractor shall mark the Specifications to indicate the actual installation where the installation varies substantially from that indicated in the Contract Specifications and modifications issued. (Note related Project Record Drawing information where applicable). The Contractor shall pay particular attention to substitutions, selection of product options, and information on concealed installations that would be difficult to identify or measure and record later. Upon completion of the mark ups, the Contractor shall submit record Specifications to the COTR. As with master relines, Contractor shall maintain record specifications for Resident Engineer review and inspection at anytime.
11. Record Product Data: The Contractor shall maintain one (1) copy of each Product Data submittal for Project Record Document purposes. The Data shall be marked to indicate the actual product installed where the installation varies substantially from that indicated in the Product Data submitted. Significant changes in the product

delivered to the site and changes in manufacturer's instructions and recommendations for installation shall be included. Particular attention will be given to information on concealed products and installations that cannot be readily identified or recorded later. Note related Change Orders and mark up of Record Construction Documents, where applicable. Upon completion of mark up, submit a complete set of Record Product Data to the COTR.

12. Miscellaneous Records: The Contractor shall maintain one (1) copy of miscellaneous records for Project Record Document purposes. Refer to other Specifications for miscellaneous record-keeping requirements and submittals concerning various construction activities. Before substantial completion, complete miscellaneous records and place in good order, properly identified and bound or filed, ready for use and reference. Categories of requirements resulting in miscellaneous records include, a minimum of the following:
    a. Certificates received instead of labels on bulk products.
    b. Testing and qualification of tradesmen. (“Contractor’s Qualifications”)
    c. Documented qualification of installation firms.
    d. Load and performance testing.
    e. Inspections and certifications.
    f. Final inspection and correction procedures.
    g. Project schedule
13. Record Construction Documents (Record As-Built)
    a. Upon project completion, the contractor shall submit the project master redlines to the Resident Engineer prior to development of Record construction documents. The Resident Engineer shall be given a minimum of a thirty (30) day review period to determine the adequacy of the master redlines. If the master redlines are found suitable by the Resident Engineer, the Resident Engineer will initial and date each sheet and turn redlines over to the contractor for as built development.
    b. The Contractor shall provide the Resident Engineer a complete set of "as-built" drawings and original master redlined marked "as-built" blue-line in the latest version of AutoCAD drawings unlocked on CD or DVD. The as-built drawing shall include security device number, security closet connection location, data

gathering panel number, and input or output number as applicable. All corrective notations made by the Contractor shall be legible when submitted to the COTR. If, in the opinion of the COTR, any redlined notation is not legible, it shall be returned to the Contractor for re-submission at no extra cost to the Owner. The Contractor shall organize the Record Drawing sheets into manageable sets bound with durable paper cover sheets with suitable titles, dates, and other identifications printed on the cover. The submitted as built shall be in editable formats and the ownership of the drawings shall be fully relinquished to the owner.

c. Where feasible, the individual or entity that obtained record data, whether the individual or entity is the installer, sub-contractor, or similar entity, is required to prepare the mark up on Record Drawings. Accurately record the information in a comprehensive drawing technique. Record the data when possible after it has been obtained. For concealed installations, record and check the mark up before concealment. At the time of substantial completion, submit the Record Construction Documents to the COTR. The Contractor shall organize into bound and labeled sets for the COTR's continued usage. Provide device, conduit, and cable lengths on the conduit drawings. Exact in-field conduit placement/routings shall be shown. All conduits shall be illustrated in their entire length from termination in security closets; no arrowed conduit runs shall be shown. Pull box and junction box sizes are to be shown if larger than 100mm (4 inch).

O. FIPS 201 Compliance Certificates

SPEC WRITER NOTE: Delete and add components to the list as required by the project. Check http://www.fips201.com/ website for list of the approved products.

1. Provide Certificates for all software components and device types utilizing credential verification. Provide certificates for:
   a. Fingerprint Capture Station
   b. Card Readers
   c. Facial Image Capturing Camera
   d. PIV Middelware
   e. Template Matcher

f. Electromagnetically Opaque Sleeve

g. Certificate Management

1) CAK Authentication System

2) PIV Authentication System

3) Certificate Validator

4) Cryptographic Module

h. <list devices and software>

P. Approvals will be based on complete submission of manuals together with shop drawings.

Q. Completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

1.5 APPLICABLE PUBLICATIONS

SPEC WRITER NOTE: Delete first paragraph below if stand alone specs. Delete rest of the subparagraphs if section 28 05 00 is provided with the project.

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

B. American National Standards Institute (ANSI)/ Security Industry Association (SIA):

AC-03	Access Control: Access Control Guideline Dye Sublimation Printing Practices for PVC Access Control Cards
TVAC-01	CCTV to Access Control Standard - Message Set for System Integration

C. American National Standards Institute (ANSI)/ International Code Council (ICC):

A117.1	Standard on Accessible and Usable Buildings and Facilities

D. Department of Justice American Disability Act (ADA)

28 CFR Part 36	ADA Standards for Accessible Design 2010

E. Department of Veterans Affairs (VA):

PACS-R: Physical Access Control System (PACS) Requirements
VA Handbook 0730 Security and Law Enforcement
F. Government Accountability Office (GAO):
GAO-03-8-02 Security Responsibilities for Federally Owned and Leased Facilities
G. National Electrical Contractors Association
303-2005 ..... Installing Closed Circuit Television (CCTV) Systems
H. National Electrical Manufactures Association (NEMA):
250-08 ..... Enclosures for Electrical Equipment (1000 Volts Maximum)
I. National Fire Protection Association (NFPA):
70-11 ..... National Electrical Code
J. Underwriters Laboratories, Inc. (UL):
294-99 ..... The Standard of Safety for Access Control System Units
305-08 ..... Standard for Panic Hardware
639-97 ..... Standard for Intrusion-Detection Units
752-05 ..... Standard for Bullet-Resisting Equipment
827-08 ..... Central Station Alarm Services
1076-95 ..... Standards for Proprietary Burglar Alarm Units and Systems
1981-03 ..... Central Station Automation System
2058-05 ..... High Security Electronic Locks
K. Homeland Security Presidential Directive (HSPD):
HSPD-12 ..... Policy for a Common Identification Standard for Federal Employees and Contractors
L. Federal Communications Commission (FCC):
(47 CFR 15) Part 15 Limitations on the Use of Wireless Equipment/Systems
M. Federal Information Processing Standards (FIPS):
FIPS-201-1 ..... Personal Identity Verification (PIV) of Federal Employees and Contractors
N. National Institute of Standards and Technology (NIST):
IR 6887 V2.1 ..... Government Smart Card Interoperability Specification (GSC-IS)
Special Pub 800-63 ..... Electronic Authentication Guideline
Special Pub 800-96 ..... PIV Card Reader Interoperability Guidelines

Special Pub 800-73-3 ... Interfaces for Personal Identity Verification (4 Parts)
..... Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation
..... Pt. 2- PIV Card Application Card Command Interface
..... Pt. 3- PIV Client Application Programming Interface
..... Pt. 4- The PIV Transitional Interfaces & Data Model Specification
Special Pub 800-76-1 ... Biometric Data Specification for Personal Identity Verification
Special Pub 800-78-2 ... Cryptographic Algorithms and Key Sizes for Personal Identity Verification
Special Pub 800-79-1 ... Guidelines for the Accreditation of Personal Identity Verification Card Issuers
Special Pub 800-85B-1 .. DRAFTPIV Data Model Test Guidelines
Special Pub 800-85A-2 .. PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 compliance)
Special Pub 800-96 ..... PIV Card Reader Interoperability Guidelines
Special Pub 800-37 ..... Guide for Applying the Risk Management Framework to Federal Information Systems
Special Pub 800-96 ..... PIV Card Reader Interoperability Guidelines
Special Pub 800-96 ..... PIV Card Reader Interoperability Guidelines
Special Pub 800-104A ... Scheme for PIV Visual Card Topography
Special Pub 800-116 .... Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

O. Institute of Electrical and Electronics Engineers (IEEE):
C62.41 ..... IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

P. International Organization for Standardization (ISO):
7810 ..... Identification cards – Physical characteristics
7811 ..... Physical Characteristics for Magnetic Stripe Cards
7816-1 ..... Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics

7816-2 ..... Identification cards - Integrated circuit cards - Part 2: Cards with contacts -Dimensions and location of the contacts

7816-3 ..... Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols

7816-4 ..... Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods

7816-10 ..... Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

14443 ..... Identification cards - Contactless integrated circuit cards; Contactless Proximity Cards Operating at 13.56 MHz in up to 5 inches distance

15693 ..... Identification cards -- Contactless integrated circuit cards - Vicinity cards; Contactless Vicinity Cards Operating at 13.56 MHz in up to 50 inches distance

19794 ..... Information technology - Biometric data interchange formats

Q. Uniform Federal Accessibility Standards (UFAS) 1984

R. ADA Standards for Accessible Design 2010

S. Section 508 of the Rehabilitation Act of 1973

1.6 DEFINITIONS

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. ABA Track: Magnetic stripe that is encoded on track 2, at 75-bpi density in binary-coded decimal format; for example, 5-bit, 16-character set.

B. Access Control List: A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person’s identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.

C. Access Control: A function or a system that restricts access to authorized persons only.
D. API Application Programming Interface
E. Assurance Level (or E-Authentication Assurance Level): A measure of trust or confidence in an authentication mechanism defined in OMB Memorandum M-04-04 and NIST Special Publication (SP) 800-63, in terms of four levels: [M-04-04]
   1. Level 1: LITTLE OR NO confidence
   2. Level 2: SOME confidence
   3. Level 3: HIGH confidence
   4. Level 4: VERY HIGH confidence
F. Authentication: A process that establishes the origin of information, or determines an entity's identity. In this publication, authentication often means the performance of a PIV authentication mechanism.
G. Authenticator: A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and fingerprints are authenticators.
H. Authorization: A process that associates permission to access a resource or asset with a person and the person's identifier(s).
I. BIO or BIO-A: A FIPS 201 authentication mechanism that is implemented by using a Fingerprint data object sent from the PIV Card to the PACS. Note that the short-hand "BIO (-A)" is used throughout the document to represent both BIO and BIO-A authentication mechanisms.
J. Biometric: An authenticator produced from measurable qualities of a living person.
K. CAC EP – CAC End Point with end point PIV applet
L. CAC NG – CAC Next Generation with transitional PIV applet
M. Card Authentication Key (CAK): A PIV authentication mechanism (or the PIV Card key of the same name) that is implemented by an asymmetric or symmetric key challenge/response protocol. The CAK is an optional mechanism defined in NIST SP 800-73. [SP800-73] NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate, and that agencies use the asymmetric CAK protocol, rather than a symmetric CAK protocol, whenever the CAK authentication mechanism is used with PACS.
N. CCTV: Closed-circuit television.

O. Central Station: A PC with software designated as the main controlling PC of the PACS. Where this term is presented with initial capital letters, this definition applies.
P. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.
Q. CPU: Central processing unit.
R. Credential: Data assigned to an entity and used to identify that entity.
S. File Server: A PC in a network that stores the programs and data files shared by users.
T. FIPS Federal Information Processing Standards
U. FRAC – First Responder Authentication Credential
V. HSPD Homeland Security Presidential Directive
W. I/O: Input/Output.
X. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.
Y. IEC International Electrotechnical Commission
Z. ISO International Organization for Standardization
AA. KB Kilobyte
BB. kbit/s Kilobits / second
CC. LAN: Local area network.
DD. LED: Light-emitting diode.
EE. Legacy CAC – Contact only Common Access Card with v1 and v2 applets
FF. Location: A Location on the network having a PC-to-Controller communications link, with additional Controllers at the Location connected to the PC-to-Controller link with RS-485 communications loop. Where this term is presented with an initial capital letter, this definition applies.
GG. NIST: National Institute of Standards and Technology
HH. PACS: Physical Access Control System
II. PC/SC: Personal Computer / Smart Card
JJ. PC: Personal computer. This acronym applies to the Central Station, workstations, and file servers.

KK. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).

LL. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.

MM. PIV: Personal Identification Verification

NN. PIV-I – PIV Interoperable credential

OO. PPS: Protocol and Parameters Selection

PP. RF: Radio frequency.

QQ. ROM: Read-only memory. ROM data are maintained through losses of power.

RR. RS-232: An TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.

SS. RS-485: An TIA/EIA standard for multipoint communications.

TT. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

UU. TPDU: Transport Protocol Data Unit

VV. TWIC – Transportation Worker Identification Credential

WW. UPS: Uninterruptible power supply.

XX. Vcc: Voltage at the Common Collector

YY. WAN: Wide area network.

ZZ. WAV: The digital audio format used in Microsoft Windows.

AAA. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

BBB. Windows: Operating system by Microsoft Corporation.

CCC. Workstation: A PC with software that is configured for specific limited security system functions.

1.7 COORDINATION

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. Coordinate arrangement, mounting, and support of electronic safety and security equipment:

1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
2. To provide for ease of disconnecting the equipment with minimum interference to other installations.

3. To allow right of way for piping and conduit installed at required slope.
4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.

B. Coordinate installation of required supporting devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.

C. Coordinate location of access panels and doors for electronic safety and security items that are behind finished surfaces or otherwise concealed.

1.8 MAINTENANCE & SERVICE

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. General Requirements

1. The Contractor shall provide all services required and equipment necessary to maintain the entire integrated electronic security system in an operational state as specified for a period of one (1) year after formal written acceptance of the system. The Contractor shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work. Impacts on facility operations shall be minimized when performing scheduled adjustments or other non-scheduled work. See also General Project Requirements.

B. Description of Work

1. The adjustment and repair of the security system includes all software updates, panel firmware, and the following new items computers equipment, communications transmission equipment and data transmission media (DTM), local processors, security system sensors, physical access control equipment, facility interface, signal transmission equipment, and video equipment.

C. Personnel

1. Service personnel shall be certified in the maintenance and repair of the selected type of equipment and qualified to accomplish all work promptly and satisfactorily. The Resident Engineer shall be advised in writing of the name of the designated service representative, and of any change in personnel. The Resident

Engineer shall be provided copies of system manufacturer certification for the designated service representative.

D. Schedule of Work

1. The work shall be performed during regular working ours, Monday through Friday, excluding federal holidays. These inspections shall include:
   a) The Contractor shall perform two (2) minor inspections at six (6) month intervals or more if required by the manufacturer, and two (2) major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.
      1) Minor Inspections shall include visual checks and operational tests of all console equipment, peripheral equipment, local processors, sensors, electrical and mechanical controls, and adjustments on printers.
      2) Major Inspections shall include all work described for Minor Inspections and the following: clean all system equipment and local processors including interior and exterior surfaces; perform diagnostics on all equipment; operational tests of the CPU, switcher, peripheral equipment, recording devices, monitors, picture quality from each camera; check, walk test, and calibrate each sensor; run all system software diagnostics and correct all problems; and resolve any previous outstanding problems.

E. Emergency Service

1. The owner shall initiate service calls whenever the system is not functioning properly. The Contractor shall provide the Owner with an emergency service center telephone number. The emergency service center shall be staffed 24 hours a day 365 days a year. The Owner shall have sole authority for determining catastrophic and non-catastrophic system failures within parameters stated in General Project Requirements.
   a. For catastrophic system failures, the Contractor shall provide same day four (4) hour service response with a defect correction time not to exceed eight (8) hours from [notification] [arrival on site]. Catastrophic system failures are defined as any system failure that the Owner determines will place the facility(s) at increased risk.

b. For non-catastrophic failures, the Contractor within eight (8) hours with a defect correction time not to exceed 24 hours from notification.

F. Operation

1. Performance of scheduled adjustments and repair shall verify operation of the system as demonstrated by the applicable portions of the performance verification test.

G. Records & Logs

1. The Contractor shall maintain records and logs of each task and organize cumulative records for each component and for the complete system chronologically. A continuous log shall be submitted for all devices. The log shall contain all initial settings, calibration, repair, and programming data. Complete logs shall be maintained and available for inspection on site, demonstrating planned and systematic adjustments and repairs have been accomplished for the system.

H. Work Request

1. The Contractor shall separately record each service call request, as received. The record shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing the action taken, the amount and nature of the materials used, and the date and time of commencement and completion. The Contractor shall deliver a record of the work performed within five (5) working days after the work was completed.

I. System Modifications

1. The Contractor shall make any recommendations for system modification in writing to the COTR. No system modifications, including operating parameters and control settings, shall be made without prior written approval from the COTR. Any modifications made to the system shall be incorporated into the operation and maintenance manuals and other documentation affected.

J. Software

1. The Contractor shall provide all software updates when approved by the Owner from the manufacturer during the installation and 12-month warranty period and verify operation of the system. These updates shall be accomplished in a timely manner, fully coordinated with the

system operators, and incorporated into the operations and maintenance manuals and software documentation. There shall be at least one (1) scheduled update near the end of the first year's warranty period, at which time the Contractor shall install and validate the latest released version of the Manufacturer's software. All software changes shall be recorded in a log maintained in the unit control room. An electronic copy of the software update shall be maintained within the log. At a minimum, the contractor shall provide a description of the modification, when the modification occurred, and name and contact information of the individual performing the modification. The log shall be maintained in a white 3 ring binder and the cover marked "SOFTWARE CHANGE LOG".

1.9 PERFORMANCE REQUIREMENTS

A. PACS shall provide support for multiple authentication modes and bidirectional communication with the reader. PACS shall provide implementation capability for enterprise security policy and incident response.

B. All processing of authentication information must occur on the "safe side" of a door

SPEC WRITER NOTE: Select facility risk levels per Facility Security Level (FSL) Determination.

C. Physical Access Control System shall provide access to following Security Areas:
   1. Controlled
   2. Limited
   3. Exclusion

D. PACS shall provide:
   1. One authentication factor for access to Controlled security areas
   2. Two authentication factors for access to Limited security areas
   3. Three authentication factors for access to Exclusion security areas

E. PACS shall provide Credential Validation and Path Validation per NIST 800-116.

F. The PACS System shall have an Enterprise Path Validation Module (PVM) component that processes X.509 certification paths composed of X.509 v3 certificates and X.509 v2 CRLs. The PVM component MUST support the following features:
   1. Name chaining;

2. Signature chaining;
3. Certificate validity;
4. Key usage, basic constraints, and certificate policies certificate extensions;
5. Full CRLs; and
6. CRLs segmented on names.

SPEC WRITER NOTE: Retain one of first two paragraphs (G or H).

G. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for physical access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.

H. Number of Locations: Support unlimited number of separate Locations using a single PC with combinations of direct-connect, dial-up, or TCP/IP LAN connections to each Location.
   1. Each Location shall have its own database and history in the Central Station. Locations may be combined to share a common database.

I. Data Capacity:
   1. [130] <Insert number> different card-reader formats.
   2. [999] <Insert number> comments.
   3. [16] <Insert number> graphic file types for importing maps.

J. Location Capacity:
   1. [128] <Insert number> reader-controlled doors.
   2. [50,000] <Insert number> total access credentials.
   3. [2048] <Insert number> supervised alarm inputs.
   4. [2048] <Insert number> programmable outputs.
   5. [32,000] <Insert number> custom action messages per Location to instruct operator on action required when alarm is received.

K. System Network Requirements:
   1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.

2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.

SPEC WRITER NOTE: Retain subparagraph below if required for system size and complexity. Add file servers and system backup Controllers if required. Show on riser diagram, and indicate size and software requirements on Drawings or in this Section.

4. Communications Controller may be used as an interface between the Central Station display systems and the field device network. Communications Controller shall provide functions required to attain the specified network communications performance.

L. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.

M. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.

SPEC WRITER NOTE: Retain optional sentence in first paragraph below only if the system is large enough where response time is a concern, and if several Locations are expected to experience heavy traffic in or out of secured areas. If retaining, add a description of the heavy load and possibly add testing requirements that include how the heavy load is simulated and how response time is to be verified.

N. System Response to Alarms: Field device network shall provide a system end-to-end response time of [1] <Insert number> second(s) or less for every device connected to the system. Alarms shall be annunciated at the Central Station within 1 second of the alarm occurring at a

Controller or device controlled by a local Controller, and within 100 ms if the alarm occurs at the Central Station. Alarm and status changes shall be displayed within 100 ms after receipt of data by the Central Station. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console.[This response time shall be maintained during system heavy load.]

O. False Alarm Reduction: The design of Central Station and Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

P. Error Detection: A cyclic code error detection method shall be used between Controllers and the Central Station, which shall detect single- and double-bit errors, burst errors of eight bits or less, and at least 99 percent of all other multibit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if one bit is received incorrectly. System shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the Central Station shall print a communication failure alarm message. System shall monitor the frequency of data transmission failure for display and logging.

Q. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

R. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the PACS. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with the controls and PC-based software and hardware in this Section.

S. References to industry and trade association standards and codes are minimum installation requirement standards.

T. Drawings and other specification sections shall govern in those instances where requirements are greater than those specified in the above standards.

1.10 EQUIPMENT AND MATERIALS

//A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//

A. Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available.

B. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer.

C. Equipment Assemblies and Components:

1. Components of an assembled unit need not be products of the same manufacturer.
2. Manufacturers of equipment assemblies, which include components made by others, shall assume complete responsibility for the final assembled unit.
3. Components shall be compatible with each other and with the total assembly for the intended service.
4. Constituent parts which are similar shall be the product of a single manufacturer.

D. Factory wiring shall be identified on the equipment being furnished and on all wiring diagrams.

E. When Factory Testing Is Specified:

1. The Government shall have the option of witnessing factory tests. The contractor shall notify the VA through the Resident Engineer a minimum of 15 working days prior to the manufacturers making the factory tests.
2. Four copies of certified test reports containing all test data shall be furnished to the Resident Engineer prior to final inspection and not more than 90 days after completion of the tests.
3. When equipment fails to meet factory test and re-inspection is required, the contractor shall be liable for all additional expenses, including expenses of the Government.

1.11 WARRANTY OF CONSTRUCTION.

A. Warrant PACS work subject to the Article “Warranty of Construction” of FAR clause 52.246-21.

B. Demonstration and training shall be performed prior to system acceptance.

1.12 GENERAL REQUIREMENTS

A. For general requirements that are common to more than one section in Division 28 refer to Section 28 05 00, REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATIONS.

B. General requirements applicable to this section include:

1. General Arrangement Of Contract Documents,
2. Delivery, Handling and Storage,
3. Project Conditions,
4. Electrical Power,
5. Lightning, Power Surge Suppression, and Grounding,
6. Electronic Components,
7. Substitute Materials and Equipment, and
8. Like Items.

PART 2 – PRODUCTS

SPEC WRITER NOTE: Delete or amend all paragraphs and sub-paragraphs as needed to ensure that only the equipment required per the Request for Proposal (RFP) is provided.

2.1 GENERAL

A. All equipment and materials for the system will be compatible to ensure correct operation as outlined in FIPS 201, March 2006 and HSPD-12.

B. The security system characteristics listed in this section will serve as a guide in selection of equipment and materials for the PACS. If updated or more suitable versions are available then the Contracting Officer will approve the acceptance of prior to an installation.

C. PACS equipment shall meet or exceed all requirements listed below.

D. A PACS shall be comprised of, but not limited to, the following components:

1. Physical Access Control System
2. Application Software
3. System Database
4. Surge and Tamper Protection
5. Standard Workstation Hardware
6. Communications Workstation
7. Controllers (Data Gathering Panel)
8. Secondary Alarm Annunciator

9. Keypads
10. Card Readers
11. Credential Cards
12. Biometric Identity Verification Equipment
13. Enrolment Center (To be provided in accordance with the VA PIV enrollment and issuance system.)
14. System Sensors and Related Equipment
15. Push Button Switches
16. Interfaces
17. Door and Gate Hardware interface
18. RS-232 ASCII Interface
19. Floor Select Elevator Control
20. After-Hours HVAC Control
21. Real Time Guard Tour
22. Video and Camera Control
23. Cables
24. Transformers

2.2 SECURITY MANAGEMENT SYSTEM (SMS)

A. Shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated client workstations or any combination of all or some.

B. Shall be expandable to support an unlimited number of individual module or integrated client workstations. All access control field hardware, including Data Gathering Panels(DGP), shall be connected to all physical access control system workstation on the network.

C. Shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system as follows.
   1. Individual reports that consist of an employee’s name, office location, phone number or direct extension, and normal hours of operation. The report shall provide a detail listing of the employee’s daily events in relation to accessing points within a facility.
   2. System reports shall be able to produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.

D. All reports shall be in a date/time format and all information shall be clearly presented. Shall be designed to allow it to work with any industry standard network protocol and topology listed below:
   1. Transmission Control Protocol (TCP)/IP
   2. Novell Netware (IPX/SPX)
   3. Banyan VINES
   4. IBM LAN Server (NetBEUI)
   5. Microsoft LAN Manager (NetBEUI)
   6. Network File System (NFS) Networks
   7. Remote Access Service (RAS) via ISDN, x.25, and standard phone lines.

E. Shall provide full interface and control of the PACS to include the following subsystems within the PACS:
   1. Public Key Infrastructure
   2. Card Management
   3. Identity and Access Management
   4. Personal Identity Verification

F. Shall have the following features or compatibilities:
   1. The ability to be operated locally or remotely via a LAN, WAN, internet, or intranet.
   2. Event and Alarm Monitoring
   3. Database Partitioning
   4. Ability to fully integrate with all other security subsystems
   5. Enhanced Monitoring Station with Split Screen Views
   6. Alternate and Extended Shunt by Door
   7. Escort Management
   8. Enhanced IT-based Password Protection
   10. N-man Rule and Occupancy Restrictions
   11. Open Journal Data Format for Enhanced Reporting
   12. Automated Personnel Import
   13. ODBC Support
   14. Windows 2000 Professional, Windows Server 2003, Windows XP Professionals for Servers, Windows 7
   15. Field-Level Audit Trail
   16. Cardholder Access Events

2.3 APPLICATION SOFTWARE

A. System Software: Based on [32] <Insert number>-bit, [Microsoft Windows] <Insert name of operating system> central-station and

workstation operating system and application software. Software shall have the following features:

1. Multiuser multitasking to allow independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface to show pull-down menus and a menu tree format.
3. Capability for future additions within the indicated system size limits.
4. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
5. Password-protected operator and smart card login and access.

SPEC WRITER NOTE: Retain paragraph below if a single point failure in the Central Station is unacceptable

B. Peer Computer Control Software: Shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.

SPEC WRITER NOTE: DTS links may be included with perimeter protection systems

C. Application Software: Interface between the alarm annunciation and entry-control Controllers, to monitor sensors[and DTS links], operate displays, report alarms, generate reports, and help train system operators. Software shall have the following functions:

1. Resides at the Central Station, workstations, and Controllers as required to perform specified functions.
2. Operate and manage peripheral devices.
3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics views to represent alarms and I/O devices.
5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.

6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
9. Automatic and encrypted backups for database and history backups shall be automatically stored at [the central control PC] [a selected workstation] and encrypted with a nine-character alphanumeric password, which must be used to restore or read data contained in backup.
10. Operator audit trail for recording and reporting all changes made to database and system software.

D. Workstation Software:
1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.
2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

E. Controller Software:
1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about physical access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.

2. Functions: The following functions shall be fully implemented and operational within each Controller:
   a. Monitoring inputs.
   b. Controlling outputs.
   c. Automatically reporting alarms to the Central Station.
   d. Reporting of sensor and output status to Central Station on request.
   e. Maintaining real time, automatically updated by the Central Station at least once a day.
   f. Communicating with the Central Station.
   g. Executing Controller resident programs.
   h. Diagnosing.
   i. Downloading and uploading data to and from the Central Station.
3. Controller Operations at a Location:
   a. Location: Up to [64] <Insert number> Controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station or workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the Central Station or workstations are off line.
   b. In the event of communications failure between the Central Station and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.
   c. Buffered events shall be handled in a first-in-first-out mode of operation.
4. Individual Controller Operation:
   a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1024 events shall be provided at each Controller.

b. Card-reader ports of a Controller shall be custom configurable for at least [120] <Insert number> different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.
e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.
h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:
   a. System shall monitor and report status of RS-485 communications loop [TCP/IP communication status] of each Location.

      SPEC WRITER NOTE: Missed polls indicate that messages had to be retransmitted and reflect the soundness or quality of the Controller-to-Controller network.

   b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.

c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

F. PC-to-Controller Communications:

1. Central-station or workstation communications shall use the following:
   a. Direct connection using serial ports of the PC.
   b. TCP/IP LAN network interface cards.
   c. Dial-up modems for connections to Locations.
2. Serial Port Configuration: Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only"; or as an ASCII output port.
3. Multiport Communications Board: Use if more than two serial ports are needed.
   a. Expandable and modular design. Use a 4-, 8-, or 16-serial port configuration that is expandable to 32 or 64 serial ports.
   b. Connect the first board to an internal PCI bus adapter card.
4. Direct serial, TCP/IP, and dial-up communications shall be alike in the monitoring or control of system, except for the connection that must first be made to a dial-up Location.

   SPEC WRITER NOTE: Poll frequency and message response time-out settings allow tuning for bandwidth and latency issues associated with network communications.

5. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.
6. PC-to-Controller and Controller-to-Controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.

G. Direct Serial or TCP/IP PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-Controller communications link.
2. Loss of communications to any Controller shall result in an alarm at all PCs running the communications software.
3. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the Controller.

H. Dial-up Modem PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-Controller communications link during dial-up modem connect times.
2. Communication software shall be programmable to routinely poll each of the remote dial-up modem Locations, collecting event logs and verifying phone lines at time intervals that are operator selectable for each Location.
3. System shall be programmable for dialing and connecting to all dial-up modem Locations and for retrieving the accrued history transactions on an automatic basis as often as once every [10] <Insert number> minutes and up to once every [9999] <Insert number> minutes.
4. Failure to communicate to a dial-up Location three times in a row shall result in an alarm at the PC.
5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the host PC will be set to, and maintained at, the proper local time. This feature shall allow for geographical time zones that are ahead of or behind the host PC.
6. The Controller connected to a dial-up modem shall automatically buffer all normal transactions until its buffer reaches 80 percent of capacity. When the transaction buffer reaches 80 percent, the Controller shall automatically initiate a call to the Central Station and upload all transactions.
7. Alarms shall be reported immediately.
8. Dial-up modems shall be provided by manufacturer of the system. Modems used at the Controller shall be powered by the Controller. Power to the modem shall include battery backup if the Controller is so equipped.

I. Controller-to-Controller Communications:

1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.

2. RS-485 communications signal shall be regenerated at each Controller.

J. Database Downloads:

1. All data transmissions from PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

SPEC WRITER NOTE: Retain subparagraph below if Project includes direct dial-up over long distances and off-peak long-distance calling is desired.

3. Software shall provide for setting downloads via dial-up connection to once per 24-hour period, with time selected by the operator.

SPEC WRITER NOTE: Retain subparagraph below if several dial-up modems are connected to a single telephone line. This prevents system from multiple sequential phone calls when editing a dial-up Locations' data.

4. Software shall provide for setting delays of database downloads for dial-up connections. Delays change the download from immediately to a delay ranging from 1 to 999 minutes.

K. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.

5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:
   a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
   b. Maps to provide real-time display animation and allow for control of points assigned to them.
   c. System to allow inputs, outputs, and override groups to be placed on different maps.
   d. Software to allow changing the order or priority in which maps will be displayed.
7. Override Groups Containing I/Os:
   a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
   b. Icon shall change automatically to show the live summary status of points in that group.
   c. Override group icon shall provide a method to manually control or set to time zone points in the group.
   d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.
8. Schedule Overrides of I/Os and Override Groups:
   a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
   b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
   c. The first time and date shall be assigned the override state that the point shall advance to, when the time and date become current.
   d. The second time and date shall be assigned the state that the point shall return to, when the time and date become current.

9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

L. Operator Access Control:
   1. Control operator access to system controls through [three] <Insert number> password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.
   2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.
   3. A minimum of [32] <Insert number> passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.
   4. The password shall not be displayed or printed.
   5. Each password shall be definable and assignable for the following:
      a. Commands usable.
      b. Access to system software.
      c. Access to application software.
      d. Individual zones that are to be accessed.
      e. Access to database.

M. Operator Commands:
   1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
   2. Command inputs shall be acknowledged and processing shall start in not less than [1] <Insert number> second(s).
   3. Tasks that are executed by operator's commands shall include the following:
      a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
      b. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.

c. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.
d. System Test: Allows the operator to initiate a system-wide operational test.
e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
f. Print reports.
g. Change Operator: Used for changing operators.
h. Security Lighting Controls: Allows the operator to remotely turn on/off security lights.
i. Display Graphics: Used to display any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
j. Run system tests.
k. Generate and format reports.
l. Request help with the system operation.
   1) Include in main menus.
   2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
   3) Provide navigation to specific topic from within the first help window.
   4) Help shall be accessible outside the applications program.
m. Entry-Control Commands:

SPEC WRITER NOTE: Revise number of times entry control in first four subparagraphs below can be changed to suit Project. Coordinate with options in "Time Zones" and "Access Levels" paragraphs in Part 2 "System Database" Article.

   1) Lock (secure) or unlock (open) each controlled entry and exit up to four times a day through time-zone programming.
   2) Arm or disarm each monitored input up to four times a day through time-zone programming.
   3) Enable or disable readers or keypads up to twice a day through time-zone programming.
   4) Enable or disable cards or codes up to four times per day per entry point through access-level programming.

4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the

command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:

a. Command entered is incorrect or incomplete.
b. Operator is restricted from using that command.
c. Command addresses a point that is disabled or out of service.
d. Command addresses a point that does not exist.
e. Command is outside the system's capacity.

N. Alarms:

SPEC WRITER NOTE: Edit paragraphs 1.a. to 1. g to suit Project. For a stand-alone access-control system, reference is to access points. Terms such as "zone," "sensor," etc., are used in other related Sections; coordinate with terms used in those Sections if alarms of these systems are integrated into this system.

1. System Setup:
   a. Assign manual and automatic responses to incoming point status change or alarms.
   b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.
   c. 60-character message field for each alarm.
   d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages. Setup shall assign messages to [access point] [zone] [sensor]<other alarm originating device>.
   e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.
   f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.
   g. Store the most recent 1000 alarms for recall by the operator using the report generator.
2. Software Tamper:
   a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful

attempts to log onto system shall generate a software tamper alarm.

b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.

c. Maintain a transcript file of the last 5000 commands entered at the each Central Station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.

d. Allow only acknowledgment of software tamper alarms.

3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.

4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.

5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.

6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.

SPEC WRITER NOTE: Retain any or all of three subparagraphs below if Project includes perimeter protection, intrusion detection, and video surveillance systems and if these systems interface with physical access control. Edit to suit Project and interface conditions.

7. Alarm Automation Interface: High-level interface to Central Station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in same manner as burglar alarms, using an RS-232 ASCII interface.

8. CCTV Alarm Interface: Allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.

9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

O. Alarm Monitoring: Monitor sensors, Controllers, and DTS circuits and notify operators of an alarm condition. Display higher-priority alarms

first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.

1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.
2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.
3. Maps shall automatically display the alarm condition for each input assigned to that map, if that option is selected for that input location.
4. Alarms initiate a status of "pending" and require the following two handling steps by operators:
   a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
   b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.
5. Each workstation shall display the total pending alarms and total unresolved alarms.
6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
7. Alarms shall transmit to Central Station in real time, except for allowing connection time for dial-up locations.
8. Alarms shall be displayed and managed from a minimum of four different windows.
   a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.
   b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.
   c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.
   d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.

9. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
10. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.
11. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.
12. Identical alarms from same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and Controllers.
14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.

P. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors shall be uniform throughout the system.
   1. Color Code:
      a. FLASHING RED: Alerts operator that a zone has gone into an alarm or that primary power has failed.
      b. STEADY RED: Alerts operator that a zone is in alarm and alarm has been acknowledged.
      c. YELLOW: Advises operator that a zone is in access.
      d. GREEN: Indicates that a zone is secure and that power is on.
   2. Graphics:
      a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.
      b. Allow I/O to be placed on graphic maps by the drag-and-drop method.
      c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on graphic map.
      d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic map associated with inputs or outputs.

e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.

SPEC WRITER NOTE: Retain either or both subparagraphs below if Project includes a video surveillance system and this system interfaces with physical access control. Edit to suit Project and interface conditions.

f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.

g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.

Q. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.

R. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.

2. Printing on Requests: An operator may request a printout of any report.

3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm [(such as door alarm, intrusion alarm, tamper alarm, etc.)] <Insert alarm types>, the type of sensor, the location, the time, and the action taken.

4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is In (Muster) Report:
    a. Emergency Muster Report: One click operation on toolbar launches report.
    b. Cardholder Report. Contain a count of persons that are "In" at a selected Location and a count with detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.
11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.
12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events or alarms only.
13. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.
    a. Initially store history on the hard disk of the host PC.
    b. Permit viewing of the history on workstations or print history to any system printer.
    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.

d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.
e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.

14. Reports shall have the following four options:
    a. View on screen.
    b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.
    c. "Save to File" with full path statement.
    d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.
15. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:
    a. Active, inactive, or future activate or deactivate.
    b. Code number, name, or imprinted card number.
    c. Group, Location, access levels.
    d. Start and stop code range.
    e. Codes that have not been used since a selectable number of days.
    f. In, out, or either status.
    g. Codes with trace designation.
16. The reports of system database shall allow options so that every data field may be printed.
17. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.

S. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.

2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes though a reader of opposite designation.
3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.
4. Timed Anti-Passback: A Controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at Controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.
6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential holder population anti-passback status to a neutral status.

T. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. PACS shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.
5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.

6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

SPEC WRITER NOTE: Delete paragraph 2.1 U if not applicable for the project.

U. Time and Attendance:
1. Time and attendance reporting shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length of the report.
2. Shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length of the report.
3. System software setup shall allow designation of selected access-control readers as time and attendance hardware to gather the clock-in and clock-out times of the users at these readers.
   a. Reports shall show in and out times for each day, total in time for each day, and a total in time for period specified by the user.
   b. Allow the operator to view and print the reports, or save the report to a file.
   c. Alphabetically sort reports on the person's last name, by Location or location group. Include all credential holders or optionally select individual credential holders for the report.

V. Training Software: Enables operators to practice system operation including alarm acknowledgment, alarm assessment, response force deployment, and response force communications. System shall continue normal operation during training exercises and shall terminate exercises when an alarm signal is received at the console.

W. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.
1. The enrollment station shall not have alarm response or acknowledgment functions.
2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.

3. The program shall provide means to disable the enrollment station when it is unattended to prevent unauthorized use.
4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
5. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:
   a. MASK: Determines a specific format that data must comply with.
   b. REQUIRED: Operator is required to enter data into field before saving.
   c. UNIQUE: Data entered must be unique.
   d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
   e. NAME ID: Data entered will be considered a unique ID for the cardholder.
6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.
9. Default card data can be programmed to speed data entry for sites where most card data are similar.
10. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.

SPEC WRITER NOTE: Retain paragraph below if visitor badge return is part of system

11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

SPEC WRITER NOTE: Retain paragraph X. if high availability and system redundancy requirement is applicable for the project.

X. System Redundancy & High Availability: The system shall provide multiple levels of communications redundancy and failover for all PACS hosted controllers, digital video recorders, and client workstations. The PACS shall be capable of automatically re-routing communications to alternate computers across the system without operator intervention.

SPEC WRITER NOTE: Retain paragraph X.1 or X.2 as applicable for the project.

1. PACS system configuration with a single application/ database server shall provide at a minimum the following redundancy and failover capability:
   a. The PACS shall provide communications redundancy and failover for network-attached devices. Each network attached device shall have one or more alternative communication sever(s) that can provide hosting in case of primary communications server failure.
   b. In case of primary communications server failure, the system shall automatically re-route network-attached devices to their designated backup communications servers to allow continuous system operations without loss of alarm and event transaction processing during failover.
   c. Network-attached devices which transition to backup communications servers, shall be able to be redirected back to their default primary servers, once the primary communications servers have been restored.
2. PACS system configuration with multiple regional application/ database servers shall provide at a minimum the following redundancy and failover capability:
   a) The PACS shall support the same level of communications redundancy and failover for network-attached devices per regional application/database server, allowable to span across regional application/database servers in the event of a regional application/database server failure.
   b) In case of a regional application/database server failure, client workstations shall be able to failover to their designated backup

regional application/database server to allow continuous system operations.

c) In case of a regional application/database server failure, upon server restoration, the ISMS shall automatically update and synchronize the regional application/database server.

d) Client workstations which transition to a backup regional application/database server, shall be able to be redirected back to their default regional application/database server, once the regional application/database server functions have been restored.

2.4 SURGE AND TAMPER PROTECTION

//A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY//

A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."
2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits" as recommended by manufacturer for type of line being protected.

B. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

SPEC WRITER NOTE: The specific size and speed of the computers is directly related to the size and complexity of the installation. The following minimum requirements are developed for a standard workstation, badging station, server or regional server, and an Enterprise server. A single server system is distinguished from an Enterprise class

server in that a single server system directly connects and controls all workstations and control panels. An Enterprise solution would use a large master server connected to regional or sub-servers which directly control their own subset of workstations and control panels.

2.5 PACS SERVER HARDWARE

SPEC WRITER NOTE: Edit PC specifications to suit Project requirements.

A. SMS Server Computer: Standard unmodified PC of modular design. The CPU word size shall be [64] <Insert number> bytes or larger; the CPU operating speed shall be at least [3.4] <Insert number> [GHz].

1. Processor family: [Intel® Xeon® E5640 (4 core, 2.66 GHz, 12MB L3, 80W)] <Insert text>.
2. Number of processors: 2
3. Memory: [12] <Insert number> GB RAM , expandable to a minimum of [192] <Insert number> GB without additional chassis or power supplies. Memory protection [Mirrored Memory, Online Spare, Advanced ECC, Memory Lock Step Mode] <Insert text>.
4. Input/Output: 2 expansions slots, Network Controller (2) 1GbE NC382i Multifunction 4 Ports.
5. Power Supply: Dual - minimum capacity of [460] <Insert number> W hot plug.
6. Real-Time Clock:
   a. Accuracy: Plus or minus 1 minute per month.
   b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
   c. Clock shall function for 1 year without power.
   d. Provide automatic time correction once every 24 hours by synchronizing clock with the Time Service Department of the U.S. Naval Observatory.
7. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
8. Parallel Port: An enhanced parallel port.
9. The server shall have a 1 GB NIC or greater network card, rated at 100/1000 MB/sec.
10. The server shall have dual [100] <Insert number> GB hard disk drives at [7200]] <Insert number> RPM.

11. The server shall have a CD / DVD combo drive.
12. The server operating system shall be either:

SPEC WRITER NOTE: Change text between /_/ as appropriate for the Project.

//a. Windows 2003 Server, 32 bit native mode, with Service Pack 2 or later with default services enabled.

b. Windows XP Professional Service Pack 2 or later and default services enabled.

c. Windows 2008.//

13. The Web Server shall be [IIS 7.0] <Insert text> or better.
14. The Database shall be [SQL Server 2005 (Express, Standard, Data Center, or Enterprise)] <Insert text>.
15. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
16. Color Monitor: [17″] or larger SVGA (1024 x 768) monitor with true color support.. The server shall have a dedicated 256 MB SVGA accelerated video card with at least 64 MB onboard RAM.
17. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
18. Mouse: Standard, compatible with the installed software.
19. Special function keyboard attachments or special function keys to facilitate data input of the following operator tasks:
    a. Help.
    b. Alarm Acknowledge.
    c. Place Zone in Access.
    d. Place Zone in Secure.
    e. System Test.
    f. Print Reports.
    g. Change Operator.
    h. <Insert operator tasks.>
20. CD-ROM Drive:
    a. Nominal storage capacity of [650] <Insert number> MB.
    b. Data Transfer Rate: [1.2] <Insert number> Mbps.
    c. Average Access Time: [150] <Insert number> ms.
    d. Cache Memory: [256] <Insert number> KB.
    e. Data Throughput: [1] <Insert number> MB/second, minimum.

SPEC WRITER NOTE: Remove paragraphs describing items not required for the Project.

21. Dot Matrix Alarm Printer:

a. Connected to the Central Station.
b. Minimum of 96 characters, standard ASCII character set based on ANSI X3.154, and with graphics capability and programmable control of top-of-form.
c. Prints in both red and black without ribbon change.
d. Adjustable sprockets for paper width up to 11 inches.
e. 80 columns per line, minimum speed of 200 characters per second.
f. Character Spacing: Selectable at 10, 12, or 17 characters per inch.
g. Paper: Sprocket-fed fan fold paper.

22. Report Printer:
a. Connected to the Central Station and designated workstations.
b. Laser printer with minimum resolution of [1200] <Insert number> dpi.
c. RAM: [2] <Insert number> MB, minimum.
d. Printing Speed: Minimum [12] <Insert number> pages per minute.
e. Paper Handling: Automatic sheet feeder with [250] <Insert number>-sheet paper cassette and with automatic feed.
f. Interface: Bidirectional parallel and universal serial bus.

SPEC WRITER NOTE: Redundant computers and associated hardware and software should be used where required by authorities having jurisdiction or if a single point failure would be unacceptable

B. Redundant Central Computer: One identical redundant central computer, connected in a hot standby, peer configuration. This computer shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant computer in near real-time. If central computer fails, redundant computer shall assume control immediately and automatically.

C. PACS controllers clustering shall support the following features:
1. Assignment of Master and alternate master controllers for cluster communication to the SMS server
2. Primary and backup communication paths to the SMS server
3. Encrypted communications
4. Up to [16]<insert number> controllers per cluster
5. Logical event linking between controllers in a cluster independent of SMS server communication

6. Asynchronous communication via TCP/IP (Polled devices shall not be acceptable)

D. UPS: Self-contained; complying with requirements in Division 26 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of [15] <Insert number> hours of operation of the central-station equipment, including 2 hours of alarm printer operation.

SPEC WRITER NOTE: Retain remainder of this Article if Division 26 Section "Static Uninterruptible Power Supply" is used for other UPS units. Coordinate UPS requirements with that Section

2. Batteries: Sealed, valve regulated, recombinant, lead calcium.
3. Accessories:
   a. Transient voltage suppression.
   b. Input-harmonics reduction.
   c. Rectifier/charger.
   d. Battery disconnect device.
   e. Static bypass transfer switch.
   f. Internal maintenance bypass/isolation switch.
   g. External maintenance bypass/isolation switch.
   h. Output isolation transformer.
   i. Remote UPS monitoring.
   j. Battery monitoring.
   k. Remote battery monitoring.
   l. <Insert accessories.>

2.6 STANDARD WORKSTATION HARDWARE

SPEC WRITER NOTE: Edit PC specifications to suit Project and software requirements

A. Workstation shall consist of a standard unmodified PC, with accessories and peripherals that configure the workstation for a specific duty.

B. Workstation Computer: Standard unmodified PC of modular design. The CPU word size shall be [32] <Insert number> bytes or larger; the CPU operating speed shall be at least [66] <Insert number> [MHz] [GHz].

1. Memory: [256] <Insert number> MB of usable installed memory, expandable to a minimum of [1024] <Insert number> MB without additional chassis or power supplies.
2. Power Supply: Minimum capacity of [250] <Insert number> W.
3. Real-Time Clock:

a. Accuracy: Plus or minus 1 minute per month.
b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
c. Provide automatic time correction once every [24 hours] <Insert number of hours or minutes> by synchronizing clock with the Central Station.

4. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
5. Parallel Port: An enhanced parallel port.
6. LAN Adapter Card: [10/100] <Insert number> Mbps PCI bus, internal network interface card.
7. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
8. Color Monitor: Not less than [17 inches (430 mm)] <Insert inches (mm)>, with a minimum resolution of [1280 by 1024] <Insert numbers> pixels, noninterlaced, and a maximum dot pitch of [0.28] <Insert number> mm. The video card shall support at least [256] <Insert number> colors at a resolution of [1280 by 1024] <Insert numbers> at a minimum refresh rate of [70] <Insert number> Hz.
9. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
10. Mouse: Standard, compatible with the installed software.
11. Disk storage shall include the following, each with appropriate controller:
    a. Minimum [10] <Insert number> GB hard disk, maximum average access time of [10] <Insert number> ms.
    b. Floppy Disk Drive: High density, 3-1/2-inch (90-mm) size.
    c. <Insert disk drives.>
12. CD-ROM Drive:
    a. Nominal storage capacity of [650] <Insert number> MB.
    b. Data Transfer Rate: [1.2] <Insert number> Mbps.
    c. Average Access Time: [150] <Insert number> ms.
    d. Cache Memory: [256] <Insert number> KB.
    e. Data Throughput: [1] <Insert number> MB/second, minimum.
13. Printer:
    a. Connected to the Central Station and designated workstations.

b. Laser printer with minimum resolution of [600] <Insert number> dpi.
c. RAM: [2] <Insert number> MB, minimum.
d. Printing Speed: Minimum [12] <Insert number> pages per minute.
e. Paper Handling: Automatic sheet feeder with [250] <Insert number>-sheet paper cassette and with automatic feed.

14. Interface: Bidirectional parallel, and universal serial bus.
15. LAN Adapter Card: [10/100] <Insert number> Mbps internal network interface card.

SPEC WRITER NOTE: Redundant controllers and associated hardware and software should be used if a single point failure would be unacceptable

C. Redundant Workstation: One identical redundant workstation, connected in a hot standby, peer configuration. This workstation shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant workstation in near real time. If its associated workstation fails, redundant workstation shall assume control immediately and automatically.

D. UPS: Self-contained, complying with requirements in Division 26 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of [6] <Insert number> hours of operation of the central-station equipment, including 2 hours of alarm printer operation.
2. Batteries: Sealed, valve regulated, recombinant, lead calcium.
3. Accessories:
   a. Transient voltage suppression.
   b. Input-harmonics reduction.
   c. Rectifier/charger.
   d. Battery disconnect device.

SPEC WRITER NOTE: First six subparagraphs below are optional accessories.

   e. Static bypass transfer switch.
   f. Internal maintenance bypass/isolation switch.
   g. External maintenance bypass/isolation switch.
   h. Output isolation transformer.
   i. Remote UPS monitoring.
   j. Battery monitoring.

k. Remote battery monitoring.

l. <Insert accessories.>

2.7 COMMUNICATIONS WORKSTATION

SPEC WRITER NOTE: Retain this Article if the Central Station will not be the communications hub.

A. Standard workstation, modified as follows:

1. <Insert number> additional RS-232-F serial ports. The CPU word size shall be [32] <Insert number> bytes or larger; the CPU operating speed shall be at least [66] <Insert number> MHz. Multiplexed serial ports shall be expandable with [8] <Insert number> character transmit and receive buffers for each port. Total buffer size shall be a minimum of [1] <Insert number> MB.

2. Redundant workstation is [not] required.

3. Printer is [not] required.

2.8 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.

B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.

D. Alarm Annunciation Controller:

1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network[with dc line supervision on each of its alarm inputs].

a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.

b. Alarm-Line Supervision:

1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal[, and for conditions as described in UL 1076 for line security equipment] [by monitoring for abnormal open, grounded, or shorted conditions] using dc change measurements. System shall initiate an alarm

in response to an abnormal current, which is a dc change of [5] [10] percent or more for longer than 500 ms.

2) Transmit alarm-line-supervision alarm to the Central Station during the next interrogation cycle after the abnormal current condition.

c. Outputs: Managed by Central Station software.

2. Auxiliary Equipment Power: A GFI service outlet inside the Controller enclosure.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personal identity verification devices, door strikes, magnetic latches, gate and door operators, and exit push-buttons.

a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.

b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.

2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.

c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

a. Data from entry-control devices; use this input to change modes between access and secure.

b. Database downloads and updates from the Central Station that include enrollment and privilege information.

3. Outputs:

a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
b. Grant or deny entry by sending control signals to portal-control devices[and mask intrusion alarm annunciation from sensors stimulated by authorized entries].
c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the Central Station.
d. Door Prop Alarm: If a portal is held open for longer than [20 seconds] [time listed in a schedule], alarm sounds.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.
   a. Store up to [1000] <Insert number> transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.

SPEC WRITER NOTE: Delete Paragraph 6 and subparagraphs if Controller power is provided from dedicated Power Supply.

6. Controller Power: NFPA 70, Class II power supply transformer, with 12- or 24-V ac secondary, backup battery and charger.
   a. Backup Battery: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full 1-year warranty and a pro rata 19-year warranty. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
   b. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.

c. Backup Power Supply Capacity: [5] [90] minutes of battery supply. Submit battery and charger calculations.

d. Power Monitoring: Provide manual dynamic battery load test, initiated and monitored at the control center; with automatic disconnection of the Controller when battery voltage drops below Controller limits. Report by using local Controller-mounted LEDs and by communicating status to Central Station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

1) Trouble Alarm: Normal power off load assumed by battery.

2) Trouble Alarm: Low battery.

3) Alarm: Power off.

2.9 PIV MIDDLEWARE

A. PIV Middleware shall provide three-factor authentication, including biometric matching using a fingerprint capture device capable of single fingerprint capture. Unit shall enable digital certificates can to be verified by security personnel using the issuer's certificate authority, SCVP, OCSP responder/repeater, orthe TSA hot list for TWIC cardholders. All cards shall be validated using FIPS-201 challenge-response protocol in order to identify forged or cloned cards. PIV Middleware solution shall validate all PIV, TWIC, NG CAC, and FRAC cards. TWIC card FASC-Ns shall also be verified against a live or cached TSA hot list.

B. PIV Middleware shall have ability to :

1. Verify cardholder identity and validates FIPS 201-compliant PIV-II, next-generation (NG) CAC, TWIC, or FRAC credentials in real-time
2. Perform three-factor authentication of cardholder using PIN, biometrics, and certificate (or serial numbers) detecting forged or cloned cards
3. Enroll FASC-N, photo, and pertinent cardholder information into PACS software
4. Automatically suspend a cardholder’s badge if his or her PIV, TWIC, or CAC card certificate serial number is on the Certificate Revocation List (CRL)
5. Upload a cardholder transaction audit trail to central database or exports it to a .csv file for centralized transaction management
6. Be compatible with biometric mobile terminal for off-site verification and enrollment

7. Re-validate imported cardholder certificates on a periodic basis via the Internet
8. Operate with commercial, off-the-shelf (COTS) FIPS 201 PIV-II and ANSI INCITS 378-compliant fingerprint capture devices
9. Revalidate imported cardholder certificates at regular intervals, ensuring that the credentials used in PACS system are backed by a valid set of digital certificates. Digital certificates are verified against local OCSP repeater/validation authority using the issuer's validation authority, or Microsoft Crypto Application Programming Interface (API) on Windows XP SP3 or Vista.
10. Certificate Manager shall fully support SCVP and OCSP for fast, online validation.
11. Provide verification of TWIC credentials against a live TSA hot list.
12. Support uploading local transactions to a central database for consolidated activity reporting. This application shall support a variety of ODBC- or ADO-compliant databases, including Oracle, SQL Server 2005, Informix, DB2, and Firebird.
13. Provide user with ability to produce canned transaction log queries as well as creating queries directly from the SQL database.

C. PIV Middleware PC requirements:
1. PIV Middleware software shall operate on Intel-based PC with minimum 1.8 GHz CPU, 1 GB RAM, 40 GB hard disk, and Microsoft Windows XP SP2 with Microsoft .NET Framework 2.0
2. Unit shall fingerprint capture devices and smart card reader.

D. PIV Middleware shall be FIPS 201 approved product.

2.10 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be [800]<insert number>ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Enclosure: Suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:
1. Indoors, controlled environment.

2. Indoors, uncontrolled environment.
3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visual[and audible] status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Shall be utilized for controlling the locking hardware on a door and allows for reporting back to the main control panel with the time/date the door was accessed, the name of the person accessing the point of entry, and its location.

F. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.

G. Shall be individually home run to the main panel.

H. Shall be installed in a manner that they comply with:
1. The Uniform Federal Accessibility Standards (UFAS)
2. The Americans with Disabilities Act (ADA)
3. The ADA Standards for Accessible Design

I. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, card and/or biometrics, card and/or pin and/or biometrics, supervised inputs, etc.). These card readers shall be available in the approved technology to meet FIPS 201, and is ISO 14443 A or B, ISO/IEC 7816 compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.

J. Shall be housed in an aluminum bezel with a wide lead-in for easy card entry.

K. Shall contain read head electronics, and a sender to encode digital door control signals.

L. LED’s shall be utilized to indicate card reader status and access status.

M. Shall be able to support a user defined downloadable off-line mode of operation (e.g. locked, unlocked), which will go in effect during loss of communication with the main control panel.

N. Shall provide audible feedback to indicate access granted/denied decisions. Upon a card swipe, two audible tones or beeps shall indicate

access granted and three tones or beeps shall indicate access denied. All keypad buttons shall provide tactile audible feedback.

O. Shall have a minimum of two programmable inputs and two programmable outputs.

P. All card readers that utilize keypad controls along with a reader and shall meet the following specifications:

1. Entry control keypads shall use a unique combination of alphanumeric and other symbols as an identifier. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII code ordinal sequence. Communications protocol shall be compatible with the local processor.

Q. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

1. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
4. Shall provide a means for users to indicate a duress situation by entering a special code.

R. PIV Contact Card Reader

1. Application Protocol Data Unit (APDU) Support: At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

2. Buffer Size: The reader must contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electrotechnical Commission (ISO/IEC) 7816-3:1997, Section 9.4.
3. Programming Voltage: PIV Readers shall not generate a Programming Voltage.
4. Support for Operating Class: PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.
5. Retrieval Time: Retrieval time[1] for 12.5 kilobytes (KB) of data through the contact interface of the reader shall not exceed 2.0 seconds.
6. Transmission Protocol: The PIV Reader shall support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.
7. Support for PPS Procedure: The reader shall support Protocol and Parameters Selection (PPS) procedure by having the ability to read character TA1 of the Answer to Reset (ATR) sent by the card as defined in ISO/IEC 7816-3:1997.

S. Contactless Smart Cards and Readers

1. Smart card readers shall read credential cards whose characteristics of size and technology meet those defined by ISO/IEC 7816, 14443, 15693.
2. The readers shall have "flash" download capability to accommodate card format changes.
3. The card reader shall have the capability of reading the card data and transmitting the data to the main monitoring panel.
4. The card reader shall be contactless and meet or exceed the following technical characteristics:
   a. Data Output Formats: FIPS 201 low outputs the FASC-N in an assortment of Wiegand bit formats from 40 – 200 bits. FIPS 201 medium outputs a combination FASC-N and HMAC in an assortment of Wiegand bit formats from 32 – 232 bits. All Wiegand formats or the upgradeability from Low to Medium Levels can be field configured with the use of a command card.

b. FIPS 201 readers shall be able to read, but not be limited to, DESfire and iCLASS cards.
c. Reader range shall comply with ISO standards 7816, 14443, and 15693, and also take into consideration conditions, are at a minimum 1″ to 2″ (2.5 – 5 cm).
d. APDU Support: At a minimum, the contactless interface shall support all card commands for contactless based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
e. Buffer Size: The reader shall contain a buffer large enough to receive the maximum size frame permitted by ISO/IEC 7816-3, Section 9.4.
f. ISO 14443 Support: The PIV Reader shall support parts (1 through 4) of ISO/IEC 14443 as amended in the References of this publication.
g. Type A and B Communication Signal Interfaces: The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.
h. Type A and B Initialization and Anti-Collision The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.
i. Type A and B Transmission Protocols: The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.
j. Retrieval Time: Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 2.0 seconds.
k. Transmission Speeds: The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64(~212 kbits/s), and configurable to allow activation/deactivation.
l. Readibility Range: The reader shall not be able to read PIV card more than 10cm(4inch) from the reader

2.11 BIOMETRIC IDENTITY VERIFICATION EQUIPMENT

A. Shall be FIPS 201 and NIST SP 800-76 compliant.
B. Shall utilize hand/palm, fingerprint, retinal, facial image, or voice verification and could be utilized as secondary authentication in

conjunction with card readers in high security area as defined by the VA. (Note: VA policy requires that the use of biometric measurements is limited to secondary authentication in high or medium security applications).

C. Shall be programmable, addressable, and hardwired directly to the main control panel and individually home run to the main control panel.
D. Shall be installed in a manner that they comply with:
   1. The Uniform Federal Accessibility Standards (UFAS)
   2. The Americans with Disabilities Act (ADA)
   3. The ADA Standards for Accessible Design
E. Shall include a means to construct individual templates or profiles based upon measurements taken from the person to be enrolled. This template shall be stored as part of the System Reference Database Files. The stored template shall be used as a comparative base by the personnel identity verification equipment to generate appropriate signals to the associated local processors.
F. Shall interface with PACS and SMS and provide the employee’s name, contact information, and point of access.
G. Shall allow for surface, flush, or pedestal mounting.
H. Shall have communications protocol in place that shall allow for communications with the SMS.
I. Shall determine when multiple attempts were made for verification, and shall automatically prompt the user for additional attempts up to a maximum of three tries. After a third failed attempt the unit shall generate an entry control alarm. This alarm will report to the SMS and the CCTV system. The camera viewpoint for where the alarm was generated shall automatically be called up onto a monitor and be recorded via the recording equipment. An alarm within the SMS shall also be generated recording, at a minimum, the date, time, and attempted point of entry.
J. Hand/Palm Geometry Verification:
   1. Shall utilize unique human hand measurements to identify authorized, enrolled personnel.
   2. During the scan process the hand geometry device, which shall allow the user’s hand to remain in full view during the scanning process, shall a three (3) dimensional measurement of the user’s hand identifying its size and shape.

3. This scan process shall start automatically once the user's hand is positioned. The hand geometry device shall be able to use either left or right hands for enrollment and verification.
4. Shall include an LED or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.
5. Shall only be updated at the unit itself and automatic updates via the SMS shall not be allowed.
6. Any significant change to the user’s hand, scars, loss of digit, or any other change that will alter the three dimension view of the hand shall require an update to the unit and SMS.
7. Shall provide an enrollment, recognition, and code/credential verification mode. The enrollment mode shall create a hand template for new personnel and enter the template into the entry control database file created for that person. Template information shall be compatible with the system application software. The operating mode shall be selectable by the system manager/operator from the central processor. When operating in recognition mode, the hand geometry device shall allow passage when the hand scan data from the verification attempt matches a hand geometry template stored in the database files. When operating in code/credential verification mode, the hand geometry device shall allow passage when the hand scan data from the verification attempt matches the hand geometry template associated with the identification code entered into a keypad; or matches the hand geometry template associated with credential card data read by a card reader.

K. Fingerprint Verification:
1. Shall use a unique human fingerprint pattern to identify authorized, enrolled personnel.
2. Shall allow the user’s hand to remain in full view during the scanning process, shall incorporate positive measures to establish that the hand or fingers being scanned by the device belong to a living human being.
3. Shall provide an optical or other type of scan of the user’s fingers. The fingerprint verification scanner shall automatically initiate the scan process provided the user’s fingers are positioned.

4. LED or other type of visual indicator displays shall provide a visual or visual and audible status indication and enrollee prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.
5. Any significant change to the user’s finger such as scars, loss of digit, or any other change that will alter the finger print shall require an update to the unit and SMS.
6. Shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control.
7. Shall respond to passage requests by generating signals to the local processor. The verification time shall be 2.0 seconds or less from the moment the finger print analysis scanner initiates the scan process until the fingerprint analysis scanner generates a response signal.
8. Shall:
   a. Provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create a fingerprint template for new personnel and enter the template into the system database file created for that person.
   b. Template information shall be compatible with the system application software.
   c. The operating mode shall be selectable by the system manager/operator from the central station.
9. When operating in recognition mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template stored in the database files.
10. When operating in code/credential verification mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template associated with the identification code. When entered into a keypad or it matches the fingerprint template associated with credential, the card data will then be recognized by the card reader.
11. Shall store template transactions involving fingerprint scans. The template match scores shall be stored in the matching personnel data file in a format compatible with the system application software, and shall be used for report generation.

SPEC WRITER NOTE: Refer to http://fips201ep.cio.gov/apl.php for list of approved products.

12. Shall be unit listed as FIPS 201 Approved product.

L. Iris Verification:

1. Shall utilize unique patterns within the human eye to identify authorized, enrolled personnel.
2. Shall use ambient light to capture an image of the iris of the person presenting themselves for identification. The resulting video image shall be compared against a stored template that was captured during the enrollment process.
3. Shall utilize a threshold for identification. The efficiency and accuracy of the device shall not be adversely affected by enrollees who wear contact lenses or eye glasses.
4. Shall provide a means for enrollees to align their eye for identification that does not require facial contact with the device.
5. Initiation for the scan should be automatic, but push-button could be provided to initiate the scan process. The device shall include adjustments to accommodate differences in enrollee height and mounting height shall be UFAS compliant.
6. The LED or other type of visual indicator displays shall provide a visual or visual and audible status indication and enrollee prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.
7. Verification time for the retinal verification unit shall be no greater that 1.5 seconds from the moment the action is initiated until a response signal has been generated.
8. Shall provide an enrollment mode, recognition mode, and code/credential verification mode:
   a. The enrollment mode shall create an iris template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software.
   b. When operating in recognition mode, the retinal verification unit shall allow passage when the retinal verification data from the verification attempt matches an iris template stored in the database files.
   c. When operating in code/credential verification mode, the iris scanner shall allow passage when the retinal verification data from the verification attempt matches the retinal verification template. This will occur when the associated information matches

the identification code entered into a keypad or matches the retinal verification template associated with the credential card data when recognized by a card reader.

9. Shall store template transactions involving retinal verifications. The template match scores shall be stored in the matching personnel data file in a file format compatible with the system application software, and shall be used for report generation.

M. Voice Verification:

1. Shall utilize unique patterns within the human speech pattern to identify authorized, enrolled personnel.
2. Shall digitize a profile of a person's speech to produce a stored model voice print, or template. Users shall record their full names utilizing their natural voice tendencies. This process shall be initiated by a push to talk button on the voice verification device.
3. Shall utilize a threshold for identification. The efficiency and accuracy of the device shall not be adversely affected by enrollees who have a speech impediment.
4. Shall provide a means for enrollees to align their voice for identification that does not require contact with the device.
5. The LED or other type of visual indicator displays shall provide a visual or visual and audible status indication and enrollee prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.
6. Verification time for the voice verification unit shall be no greater that 1.5 seconds from the moment the action is initiated until a response signal has been generated.
7. Shall provide an enrollment mode, recognition mode, and code/credential verification mode:
   a. The enrollment mode shall create a voice template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software.
   b. When operating in recognition mode, the voice verification unit shall allow passage when the voice verification data from the verification attempt matches a voice template stored in the database files.
   c. When operating in code/credential verification mode, the voice verifier shall allow passage when the voice verification data

from the verification attempt matches the voice verification template. This will occur when the associated information of the identification code entered into a keypad matches the voice verification template associated with a credential card data is recognized by a card reader.

8. Shall store template transactions involving voice verifications. The template match scores shall be stored in the matching personnel data file in a file format compatible with the system application software, MPEG or equivalent, and shall be used for report generation.

2.11 KEYPADS

SPEC WRITER NOTE: Scrambled keypad should be specified for very high security needs. Specify the reduced viewing angle for scrambled keypads.

A. Designed for use with unique combinations of alphanumeric and other symbols as an Identifier. Keys of keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in [ascending ASCII-code ordinal sequence] [random scrambled order]. Communications protocol shall be compatible with Controller.

1. Keypad display or enclosure shall limit viewing angles of the keypad as follows:
   a. Maximum Horizontal Viewing Angle: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.
   b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.
2. Duress Codes: Provide duress situation indication by entering a special code.

2.12 CREDENTIAL CARDS

A. Personal Identity Verification (PIV) credential cards shall comply to Federal Information Processing Standards Publication (FIPS) 201.

B. Visual Card Topography shall be compliant with NIST 800-104.

C. PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements shall collectively comprise the data model for PIV logical credentials, and include the following:

1. CHUID

2. PIN

SPEC WRITER NOTE: Delete between // and edit text below as required for the project.

3. //PIV authentication data (one asymmetric key pair and corresponding certificate)
4. + Two biometric fingerprints//.

D. The credential card (PIV) shall be an ISO 14443 type smart card with contactless interface that operates at 13.56 MHZ.

E. //The credential card (PIV) shall be an ISO 7816 type smart card.//

2.13 SYSTEM SENSORS AND RELATED EQUIPMENT

A. The PACS (Physical Access Control System) and related Equipment provided by the Contractor shall meet or exceed the following performer specifications:

B. Request to Exit Detectors:

1. Passive Infrared Request to Exit Motion Detector (REX PIR) (1) The Contractor shall provide a surface mounted motion detector to signal the physical access control system request to exit input. The motion detector shall be a passive infrared sensor designed for wall or ceiling mounting 2134 to 4572 mm (7 to 15 ft) height. The detector shall provide two (2) form “C” (SPDT) relays rated one (1) Amp. @ 30 VDC for DC resistive loads. The detectors relays shall be user adjustable with a latch time from 1-60 seconds. The detector shall also include a selectable relay reset mode to follow the timer or absence of motion. The detection pattern shall be adjustable plus or minus fourteen (± 14) degrees. The detector shall operate on 12 VDC with approximately 26 mA continuous current draw. The detector shall have an externally visible activation LED. The motion detector shall measure approximately 38 mm H x 158 mm W x 38 mm D (1.5 x 6.25 x 1.5 in). The detector shall be immune to radio frequency interference. The detector shall not activate or set-up on critical frequencies in the range 26 to 950 Megahertz using a 50 watt transmitter located 30.5 cm (1 ft) from the unit or attached wiring. The detector shall be available on gray or black enclosures. The color of the housing shall be coordinated with the surrounding surface.

C. Guard tour stations:

1. The guard tour station shall be single gang brushed steel plate flush mounted in a single gang box. The switch shall be a normally open momentary keyed switch.

D. Delayed Egress (DE)

1. General:

a. The delay egress locking hardware shall provide a method to secure emergency exits and provide an approved delayed emergency exit method. The package shall be Underwriters Laboratories listed as a delay egress-locking device. The delay egress device shall be available to support configurations with both rated and non-rated fire doors. The delay egress device shall comply with Life Safety Codes (NFPA-101, BOCA) as it applies to special locking arrangements for delay egress locks. Unless specifically identified as a non-fire rated opening, all doors shall be equipped with fire rated door hardware. The Contractor shall be responsible for providing all equipment and installation to provide a fully functioning system. Need to amend to use crashbars type mechanical release switches.

2. The delay-locking device shall include all of the following features:

a. Delay Egress Mode

1) The delayed egress device shall be a SDC 101V Series Exit Check with wall mounted control module. Upon activation of an approved panic bar the delay locking device shall begin a delay sequence of 30 seconds; a flush mounted wall LED panel adjacent to the door will indicate initiation of the countdown time. During the 30 second delay period, a local sounding device shall annunciate a tone activation of the delay cycle and verbal exit instructions. At the end of the delay cycle the locking device shall unlock and allow free egress. The reset of the local sounding device shall be user definable and include options to select either local sound until silenced by reset or local sounder silenced upon opening of the door. Unless otherwise indicated the local delay sounder shall be silenced upon opening of the door. The SDC’s device trigger output shall be connected to the SMS DGP alarm panel for pre-activation warning. The contractor shall specify the bond sensor option when ordering the delayed egress hardware; this

output shall be wired to the SMS DGP to activate an alarm if the door does not lock. Use of reset panel not top mounted device.

2) Delayed egress doors will have bond sensors.

3) Delayed egress activation shall also trigger CCTV call –up.

b. Fire Alarm Mode

1) Upon activation of the facility’s fire evacuation and water flow alarm signal the delay locking devices shall immediately unlock and provide free egress. The Contractor shall provide any required fire alarm relays or interface devices.

c. Reset Mode

1) The delay egress device shall be manually reset by the Delayed Egress controller located at the door via key switch.

2) The delay egress device shall automatically reset upon fire alarm system reset.

3) The delayed egress shall be resettable through the SMS.

d. The Contractor shall provide a Master Open Switch for all the facility’s delayed egress hardware, with protective cover and permanent labeling in the Unit Control Room. The switch shall be wired into the fire alarm system to activate the evacuation alarms. When the switch is pressed all delayed egress or evacuation doors shall unlock and generate an alarm at the security console monitor showing and recording time and date of when the switch was pressed. The contractor is responsible for coordinating the wiring and connection with the fire alarm contactor. The Master Open Switch shall be linked to the fire alarm panel for the release of doors locks.

e. Each individual delayed egress door shall have the ability to unlock through a manual action on the SMS.

f. Unless otherwise indicated the Contractor shall provide all of the above reset methods for each door. All signs will meet the latest ADA requirements.

g. Signs

1) The delay egress package shall be provided with a warning sign complying with local code requirements. The warning sign shall be attached to the interior side of the controlled door. The sign shall be located on the interior side of the door

above and within 304 mm (12 in) of the panic bar. The sign shall read:
EMERGENCY EXIT.
PUSH UNTIL
ALARM SOUNDS
DOOR CAN BE OPENED,
IN 30 SECONDS.

2) Signs shall be coordinated and comply with the building's existing sign specifications. Signs shall include grade 2 Braille.
3) Signs shall meet the current ADA requirements.
4) In instances of code and specification conflicts, the life safety code requirement shall prevail.
5) The Division 10 Contractor shall provide samples for approval with their submittal package.

3. Physical Access Control Interface
   a. The delay egress device shall be capable of interface with card access control systems.
   b. The system shall include a bypass feature that is activated via a dry contact relay output from the physical access control system. This bypass shall allow authorized personnel to pass through the controlled portal without creating an alarm condition or activating the delay egress cycle. The bypass shall include internal electronic shunts or door switches to prevent activation (re-arming) until the door returns to the closed position. An unused access event shall not cause a false alarm and shall automatically rearm the delay egress lock upon expiration of the programmed shunt time. The delay egress physical access control interface shall support extended periods of automated and/or manual lock and unlock cycles.

E. Crash Bar:
   1. Emergency Exit with Alarm (Panic):
      a. Entry control portals shall include panic bar emergency exit hardware as designed.
      b. Panic bar emergency exit hardware shall provide an alarm shunt signal to the PACS and SMS.

c. The panic bar shall include a conspicuous warning sign with one (1) inch (2.5 cm) high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.
d. Operation of the panic bar hardware shall generate an intrusion alarm that reports to both the SMS and Intrusion Detection System. The use of a micro switch installed within the panic bar shall be utilized for this.
e. The panic bar shall utilize a fully mechanical connection only and shall not depend upon electric power for operation.
f. The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications.
g. Normal Exit:
    1) Entry control portals shall include panic bar non-emergency exit hardware as designed.
    2) Panic bar non-emergency exit hardware shall be monitored by and report to the SMS.
    3) Operation of the panic bar hardware shall not generate a locally audible or an intrusion alarm within the IDS.
    4) When exiting, the panic bar shall depend upon a mechanical connection only. The exterior, non-secure side of the door shall be provided with an electrified thumb latch or lever to provide access after the credential I.D. authentication by the SMS.
    5) The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications. The strikes/bolts shall include a micro switch to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. The signal switches shall report a forced entry to the system in the event the door is left open or accessed without the identification credentials.

F. Key Bypass:
1. Shall be utilized for all doors that have a mortise or rim mounted door hardware.

2. Each door shall be individually keyed with one master key per secured area.
3. Cylinders shall be six (6)-pin and made of brass or equivalent. Keys for the cylinders shall be constructed of solid material and produced and cut by the same distributor. Keys shall not be purchased, cut, and supplied by multiple dealers.
4. All keys shall have a serial number cut into the key. No two serial numbers shall be the same.
5. All keys and cylinders shall be stored in a secure area that is monitored by the Intrusion Detection System.

G. Automatic Door Opener and Closer:
1. Shall be low energy operators.
2. Door closing force shall be adjustable to ensure adequate closing control.
3. Shall have an adjustable back-check feature to cushion the door opening speed if opened violently.
4. Motor assist shall be adjustable from 0 to 30 seconds in five (5) second increments. Motor assist shall restart the time cycle with each new activation of the initiating device.
5. Unit shall have a three-position selector mode switch that shall permit unit to be switched “ON” to monitor for function activation, switched to “H/O” for indefinite hold open function or switched to “OFF,” which shall deactivate all control functions but will allow standard door operation by means of the internal mechanical closer.
6. Door control shall be adjustable to provide compliance with the requirements of the Americans with Disabilities Act (ADA) and ANSI standards A117.1.
7. All automatic door openers and closers shall:
   a. Meet UL standards.
   b. Be fire rated.
   c. Have push and go function to activate power operator or power assist function.
   d. Have push button controls for setting door close and door open positions.
   e. Have open obstruction detection and close obstruction detection built into the unit.

f. Have door closer assembly with adjustable spring size, back-check valve, sweep valve, latch valve, speed control valve and pressure adjustment valve to control door closing.

g. Have motor start-up delay, vestibule interface delay; electric lock delay and door hold open delay up to 30 seconds. All operators shall close door under full spring power when power is removed.

h. Are to be hard wired with power input of 120 VAC, 60Hz and connected to a dedicated circuit breaker located on a power panel reserved for security equipment.

H. Door Status Indicators:

1. Shall monitor and report door status to the SMS.

2. Door Position Sensor:

a. Shall provide an open or closed indication for all doors operated on the PACS and report directly to the SMS.

b. Shall also provide alarm input to the Intrusion Detection System for all doors operated by the PACS and all other doors that require monitoring by the intrusion detection system.

c. Switches for doors operated by the PACS shall be double pole double throw (DPDT). One side of the switch shall monitor door position and the other side if the switch shall report to the intrusion detection system. For doors with electromagnetic locks a magnetic bonding sensor (MBS) can be used in place of one side of a DPDT switch, in turn allowing for the use of a single pole double throw (SPDT) switch in it place of a DPDT switch.

d. Switches for doors not operated by the PACS shall be SPDT and report directly to the IDS.

e. Shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2″ (5 cm).

2.14 PUSH BUTTON SWITCHES

A. Push-Button Switches: Momentary-contact back-lighted push buttons, with stainless-steel switch enclosures.

1. Electrical Ratings:

a. Minimum continuous current rating of [10] <Insert number> A at 120 V ac or [5] <Insert number> A at 240-V ac.

b. Contacts that will make 720 VA at [60] <Insert number> A and that will break at 720 VA at [10] <Insert number> A.

2. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.
3. Enclosures shall additionally be suitable for installation in the following locations:

SPEC WRITER NOTE: Edit location.s listed below to suit Project. Coordinate with "Environmental Conditions" Paragraph in Part 1 "Project Conditions" Article

a. Indoors, controlled environment.
b. Indoors, uncontrolled environment.
c. Outdoors.

4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.15 PORTAL CONTROL DEVICES

A. Shall be used to assist the PACS.
B. Such devices shall:
1. Provide a means of monitoring the doors status.
2. Allow for exiting a space via either a push button, request to exit, or panic/crash bar.
3. Provide a means of override to the PACS via a keypad or key bypass.
4. Assist door operations utilizing automatic openers and closures.
5. Provide a secondary means of access to a space via a keypad.
C. Shall be connected to and monitored by the main PACS panel.
D. Shall be installed in a manner that they comply with:
1. The Uniform Federal Accessibility Standards (UFAS)
2. The Americans with Disabilities Act (ADA)
3. The ADA Standards for Accessible Design
E. Shall provide a secondary means of physical access control within a secure area.
F. Push-Button Switches:
1. Shall be momentary contact, back lighted push buttons, and stainless steel switch enclosures for each push button as shown. Buttons are to be utilized for secondary means of releasing a locking mechanism.
a. In an area where a push button is being utilized for remote access of the locking device then no more than two (2) buttons shall operate one door from within one secure space. Buttons will not be wired in series with one other.
b. In an area where locally stationed guards control entry to multiple secure points via remote switches. An interface board

shall be designed and constructed for only the amount of buttons it shall house. These buttons shall be flush mounted and clearly labeled for ease of use. All buttons shall be connected to the PACS and SMS system for monitoring purposes.

c. Shall have double-break silver contacts that will make 720 VA at 60 amperes and break 720 VA at 10 amperes.

G. Entry Control Devices:

1. Shall be hardwired to the PACS main control panel and operated by either a card reader or a biometric device via a relay on the main control panel.
2. Shall be fail-safe in the event of power failure to the PACS system.
3. Shall operate at 24 VCD, with the exception of turnstiles and be powered by a separate power supply dedicated to the door control system. Each power supply shall be rated to operate a minimum of two doors simultaneously without error to the system or overload the power supply unit.
4. Shall have a diode or metal-oxide veristor (MOV) to protect the controller and power supply from reverse current surges or back-check.
5. Electric Strikes/Bolts: Shall be:
   a. Made of heavy-duty construction and tamper resistant design.
   b. Tested to over one million cycles.
   c. Rated for a minimum of 1000 lbs. holding strength.
   d. Utilize an actuating solenoid for the strike/bolt. The solenoid shall move from fully open to fully closed position and back in not more than 500 milliseconds and be rated for continuous duty.
   e. Utilize a signal switch that will indicate to the system if the strike/bolt is not engaged or is unlocked when it should be secured.
   f. Flush mounted within the door frame.

SPEC WIRTER NOTE: Electric Mortise Locks shall be provided by the Division 8 “DOOR HARDWARE” contractor. Delete between //__// if not applicable for the project.

6. Electric Mortise Locks: Shall be installed within the door and an electric transfer hinge shall be utilized to allow the wires to be transferred from the door frame to the lock. If utilized with a double door then the lock shall be installed inside the active leaf. Electric Mortise Locks shall:

a. These locks shall be provided and installed by the Division 8 “DOOR HARDWARE” Contractor.

//b. Have integrated Request to Exit switch for //new// doors receiving physical access control devices.//

b. Provide integration of the Electric Mortise Locks with the PACS for:

1) Lock Power

//2) Request to Exit switch.//

SPEC WIRTER NOTE: Electromagnetic Locks shall be provided by the Division 8 “DOOR HARDWARE” contractor. Delete between //__// if not applicable for the project.

7. Electromagnetic Locks:

a. These locks shall be without mechanical linkage utilizing no moving parts, and securing the door to its frame solely on electromagnetic force.

b. Shall be comprised of two pieces, the mag-lock and the door plate. The electromagnetic locks shall be surface mounted to the door frame and the door plate shall be surface mounted to the door.

c. Ensure a diode is installed in line with the DC voltage supplying power to the unit in order to prevent back-check on the system when the electromagnetic lock is powered.

//d. Shall utilize a magnetic bonding sensor (MBS) to monitor the door status and report that status to the SMS.//

SPEC WRITER NOTE: Magnetic bond sensor shall not be used in high security applications. Specify the Balanced magnetic switch for door status monitoring.

e. Electromagnetic locks shall meet the following minimum technical characteristics:

Operating Voltage		24 VDC
Current Draw		.5A
Holding Force	Swing Doors	675 kg (1500 lbs)
	Sliding Doors	225 kg (500 lbs)

8. Turnstiles:

a. Shall operate at 110 VAC, 60 Hz or 220 VAC, 50 Hz supplied from a dedicated circuit breaker on a security power panel. This device does not require a back-up power source.

b. Shall be utilized as a means of monitoring and controlling access in a lobby.

c. Shall meet the following minimum requirements:

1) Be UFAS compliant.

2) Provide either an audible or visual confirmation that access has been granted to a cleared individual.

3) Provide an audible alarm in the event a non-cleared individual is attempting to gain access.

4) Interface with the SMS and utilize a card reader for accessing and exiting a facility, and provide a recorded event of personnel accessing these points.

5) Have a built-in step-down transformer to provide power to a card reader unit.

6) Have built-in signal wiring chassis to allow for plug and play capabilities with the PACS.

7) Have the ability to detect tailgating within one quarter on an inch to prevent unauthorized access to a facility.

SPEC WRITER NOTE: Show vehicle gate and access-control arrangements on Drawings.

9. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers. Vehicle gate and accessories are specified in Division 32 Section "Chain Link Fences and Gates."

2.16 SECONDARY ALARM ANNUNCIATOR

SPEC WRITER NOTE: Retain this Article if system includes one or more secondary alarm annunciation consoles; coordinate with Drawings.

A. Secondary Alarm Annunciation Site: A workstation with limited I/O capacity, consisting of a secondary alarm annunciation workstation [to allow the operator to duplicate functions of the main operator interface, and to show system status changes] [to display alarms or system status changes only].

SPEC WRITER NOTE: Edit paragraphs describing the PIV Middleware to provide features of the product compatible with PACS Software/Hardware.

2.17 INTERFACES

A. CCTV System Interface

1. An RS232 [Ethernet] interface associated driver, and controller shall be provided for connection of the SMS Central Computer to the CCTV Alarm interface and switcher. The interface shall provide alarm data to the CCTV Alarm interface for automatic camera call-up. If required the Security Contractor shall be responsible for programming the command strings into the SMS Server.

B. Intercom System Interface

1. The CCTV call-up from intercom stations shall be through the intercom unit via RS232 [Ethernet] communications interface to the SMS system, then through the matrix switcher.
   a. Application Software
      1) Provides the interface between the Alarm Annunciation System and Operator; all sensors, local processors and data links, drive displays, report alarms, and report generation.
      2) Software is categorized as System Software and Application Software. System Software must consist of software to support set-up, operation, hard drive back-ups and maintenance processor. Application Software must consist of software to provide the completion of Physical Access Control System.

C. Power Supplies:

1. Shall be UL rated and able to adequately power (enter number) entry control devices on a continuous base without failure.
2. Shall meet the following minimum technical characteristics:

SPEC WRITER NOTE: Provide technical characteristics for each power supply type required; PACS panel power supply, locks power supply, rack mounted power supplies where required etc. Replace between [_] with appropriate values.

INPUT POWER	110 VAC 60 HZ (enter amperage)A
OUTPUT VOLTAGE	12 VDC Nominal (13.8 VDC) 24 VDC Nominal (27.6 VDC) Filtered and Regulated
BATTERY	Dependant on Output Voltage shall provide up to <__> Ah
OUTPUT CURRENT	[10] amp max. [@ 13.8] VDC [5] amp max. [@ 27.6] VDC
PRIMARY FUSE SIZE	6.3 amp (non-removable)

BATTERY FUSE SIZE	12 amp, 3AG
CHARGING CIRCUIT	Built-in standard

2.18 FLOOR SELECT ELEVATOR CONTROL

SPEC WRITER NOTE: Establish number of outputs with the elevator control specifications. Typical elevator interface will require one output per elevator car per floor controlled. Some systems may require one additional output per elevator bank to place elevators in after-hours mode. Specify elevator travel cable in the elevator section. Alternatively, cable may be added to this Article; if added, coordinate with elevator specifications.

A. Elevator access control shall be integral to security access.
   1. System shall be capable of providing full elevator security and control through dedicated Controllers without relying on the control-station host PC for elevator control decisions.
   2. Access-control system shall enable and disable car calls on each floor and floor select buttons in each elevator car, restricting passengers' access to the floors where they have been given access.
   3. System setup shall, through programming, automatically secure and unsecure each floor select button of a car individually by time and day. Each floor select button within a car shall be separately controlled so that some floors may be secure while others remain unsecure.
   4. When a floor select button is secure, it shall require the passenger to use his/her access code and have access to that floor before the floor select button will operate. The passenger's credential shall determine which car call and floor select buttons are to be enabled, restricting access to floors unless authorized by system's access code database. Floor select button shall be enabled only in the car where the credential holder is the passenger.

B. PACS shall record which call button is pressed, along with credential and time information.
   1. System Controller shall record elevator access data.
   2. The Controller shall reset all additional call buttons that may have been enabled by the user's credential.

3. The floor select elevator control shall allow for manual override either individually by floor or by cab as a group from a workstation PC.

2.19 AFTER-HOURS HVAC CONTROL

A. After-Hours HVAC Control: Provide for any credential read to activate or control individual HVAC zones based on access level. This control module shall control and record the after-hours use of the heating and cooling system in zones or tenant space.
   1. This control shall give the administrator the ability to determine how much extra energy consumption each tenant is responsible for. This information can be used in billing tenants for the extra after-hour usage.
   2. At the specified time every day, the HVAC shall automatically go into its after-hours mode. It shall then revert into its normal business hours mode by a tenant using an access code or card at a designated keypad or reader.
   3. Once enabled, the tenant's HVAC zone shall be under thermostat control for a preset amount of time. When the preset amount of time elapses, the HVAC for that zone shall revert back to after-hours mode unless a tenant uses his/her code or card again. This shall continue until the unit automatically returns to its normal business hours operation.

B. Control module activates the HVAC system after a valid access by any of three methods; however, the HVAC control shall always allow for manual override from the PC.
   1. By time expiration after access of an adjustable period from 1 second to 546 minutes (9.1 hours).
   2. By use of the card or code again at the same or different reader or keypad.
   3. By system returning to its normal business hours operation.

C. After-hours HVAC control shall operate with all other features running simultaneously and use the central-station PC that controls access for the building but shall not rely on the host PC for any HVAC control decisions.

2.20 REAL TIME GUARD TOUR

A. Guard tour module shall provide the ability to plan, track, and route tours. Module shall input an alarm during tour if guard fails to make

a station. Tours can be programmed for sequential or random tour-station order.

1. Guard tour setup shall define specific routes or tours for the guard to take, with time restrictions in which to reach every predefined tour station.
2. Guard tour activity shall be automatically logged to the central-station PC's hard drive.
3. If the guard is early or late to a tour station, a unique alarm per station shall appear at the Central Station to indicate the time and station.
4. Guard tour setup shall allow the tours to be executed sequentially or in a random order with an overall time limit set for the entire tour instead of individual times for each tour station.
5. Setup shall allow recording of predefined responses that will display for the operator at the control station should a "Failed to Check-in" alarm occur.

B. A tour station is a physical location a guard shall reach and perform an action indicating that the guard has arrived. This action, performed at the tour station, shall be 1 of 13 different events with any combination of station types within the same tour. A tour station shall be one of the following event types:

1. Access Granted.
2. Access Denied Code.
3. Access Denied Card plus PIN.
4. Access Denied Time Zone.
5. Access Denied Level.
6. Access Denied Facility.
7. Access Denied Code Timer.
8. Access Denied Anti-Passback.
9. Access Granted Passback Violation.
10. Alarm.
11. Restored.
12. Input Normal.
13. Input Abnormal.

C. Guard tour and other system features shall operate simultaneously with no interference.

D. Guard Tour Module Capacity: 999 possible guard tour definitions with each tour having up to 99 tour stations. System shall allow all 999 tours to be running at same time.

2.21 VIDEO AND CAMERA CONTROL

A. Control station or designated workstation displays live video from a CCTV source.

1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom command auxiliary controls.
2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.

B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For CCTV sources that are connected to a video switcher, control station shall automatically send control commands through a COM port to display the requested camera when the camera icon is selected.

C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

2.22 WIRES AND CABLES

SPEC WRITER NOTE: If stand alone specs erase between // //. If spec section 280513 is not provided for the project leave paragraphs below A-V.

//A. Refer to section 280513 "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY".//

SPEC WRITER NOTE: In this Article, coordinate the guidelines in the editor's notes for cable application with security system manufacturer's written recommendations.

A. Comply with Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."

SPEC WRITER NOTE: RS-232 communications require 3 conductors with an overall shield and a distance limitation of 50 feet (15 m).

B. PVC-Jacketed, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; PVC jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

C. Plenum-Type, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; plastic jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

D. RS-485 communications require 2 twisted pairs, with a distance limitation of 4000 feet (1220 m).

E. PVC-Jacketed, RS-485 Cable: Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

F. Plenum-Type, RS-485 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

SPEC WRITER NOTE: Retain one of first two paragraphs and associated subparagraphs below or allow Contractor to choose. First paragraph allows use of multiconductor cables instead of a separate cable for each reader or keypad; if retaining, adjust the remaining paragraphs that refer to readers and keypads to allow use of multiconductor cables. Retain uniform shielding characteristics or differentiate on Drawings where 100 percent shielding is required or where less shielding is allowed. Select insulating materials based on engineer's preference, considering manufacturer's written recommendations. When revising cable paragraphs pertaining to readers and keypads, verify that the new combination of conductor size, insulation material,

shielding, and jacket is commercially available.
The connection of card to the Controller requires a 3-pair, No. 22 or 20 AWG cable with an overall braided shield. Maximum distance from controller to reader is 250 feet (76 m) with No. 22 AWG wire, and 500 feet (152 m) with No. 20 AWG wire. The three pairs provide one pair for power, one pair for data, and one pair for two separate LED control lines. Readers with a buzzer or other options require additional conductors.

G. Multiconductor, Readers and Wiegand Keypads Cables: No. 22 AWG, paired and twisted multiple conductors, stranded (7x30) tinned copper conductors, semirigid PVC insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage, plus tinned copper braid shield with 65 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CMG.
   2. Flame Resistance: UL 1581 Vertical Tray.
   3. For TIA/EIA-RS-232 applications.

H. Paired Readers and Wiegand Keypads Cables: Paired, 3 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

I. Paired Readers and Wiegand Keypads Cable: Paired, 3 pairs, twisted, No. 20 AWG, stranded (7x28) tinned copper conductors, polyethylene (polyolefin) insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded (19x34) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

J. Plenum-Type, Paired, Readers and Wiegand Keypads Cable: Paired, 3 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum foil-polypropylene tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

K. Plenum-Type, Multiconductor, Readers and Keypads Cable: 6 conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

SPEC WRITER NOTE: Coordinate four paragraphs and associated subparagraphs below with power requirements of locks specified in Division 08. Lock wire size recommendations are for the power draw of 500 mA or less, with an inrush current of not more than 1 A. 12- to 24-V lock wire from controller to door requires a 2-conductor cable. Maximum distance from controller to lock is 250 feet (76 m) with No. 18 AWG wire, and 500 feet (152 m) with No. 16 AWG wire.

L. Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

1. NFPA 70, Type CMG.
2. Flame Resistance: UL 1581 Vertical Tray.

M. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

N. Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

1. NFPA 70, Type CMG.
2. Flame Resistance: UL 1581 Vertical Tray.

O. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

SPEC WRITER NOTE: Input cable in two paragraphs and associated subparagraphs below connects monitored device to Controller. Input requires a 2-conductor, No. 22 AWG cable; distance limitation is 1000 feet (305 m) maximum.

Cable shielding is optional but required for UL-labeled systems.

P. Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, overall aluminum foil-polyester tape shield with No. 22 AWG, stranded (7x30) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CMR.
   2. Flame Resistance: UL 1666 Riser Flame Test.

Q. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

SPEC WRITER NOTE: AC transformer cable in first two paragraphs and associated subparagraphs below connects the power transformer to the Controller if the transformer is remotely mounted from the Controller. The AC transformer cable requires a single pair cable with a maximum distance of 25 feet (8 m) for 18 AWG cable.

R. Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (7x26) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
   1. NFPA 70, Type CMG.

S. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

T. Elevator Travel Cable: Steel center core, with shielded, twisted pairs, No. 20 AWG conductor size.
   1. Steel Center Core Support: Preformed, flexible, low-torsion, zinc-coated, steel wire rope; insulated with 60 deg C flame-resistant PVC and covered with a nylon or cotton braid.
   2. Shielded Pairs: Insulated copper conductors; color-coded, insulated with 60 deg C flame-resistant PVC; each pair shielded with bare copper braid for 85 percent coverage.
   3. Jute Filler: Electrical grade, dry.
   4. Binder: Helically wound synthetic fiber.

5. Braid: Rayon or cotton braid applied with 95 percent coverage.
6. Jacket: 60 deg C PVC specifically compounded for flexibility and abrasion resistance. UL VW-1 and CSA FT1 flame rated.

SPEC WRITER NOTE: LAN cable in paragraph below is used for PC-to-PC communications.

U. LAN (Ethernet) Cabling: Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."

PART 3 - EXECUTION

3.1 GENERAL

A. The Contractor shall install all system components and appurtenances in accordance with the manufacturers' instructions, ANSI C2, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signals, communications, and data transmission lines grounding shall be installed as necessary to preclude ground loops, noise, and surges from affecting system operation. Equipment, materials, installation, workmanship, inspection, and testing shall be in accordance with manufacturers' recommendations and as modified herein.

B. Consult the manufacturers' installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the Riser/Connection diagram for all schematic system installation/termination/wiring data.

C. All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., sensors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

3.2 CURRENT SITE CONDITIONS

A. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions which will affect performance of the system to the Owner in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Owner.

3.3 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations,

installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.4 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.

1. Record setup data for control station and workstations.
2. For each Location, record setup of Controller features and access requirements.
3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
4. Set up groups, linking, and list inputs and outputs for each Controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours and key control.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.
13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.
15. Develop cable and asset management system details; input data from construction documents. Include system schematics and Technical Drawings.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.5 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."

B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

SPEC WRITER NOTE: Retain one of first two paragraphs below.

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

D. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

E. Install LAN cables using techniques, practices, and methods that are consistent with Category 5E rating of components and that ensure Category 5E performance of completed and linked signal paths, end to end.

F. Install cables without damaging conductors, shield, or jacket.

G. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

H. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.6 CABLE APPLICATION

SPEC WRITER NOTE: This Article provides examples of application requirements for cables. Edit to select cabling methods for various environments in Project. Add other methods if required. Revise conductor insulation, jacketing, and cable type designations to suit Project condition, local code, and practice.

Refer to NFPA 70 for additional application information about insulation temperature ratings in cables, and product-use classifications and restrictions

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. RS-232 Cabling: Install at a maximum distance of 50 feet (15 m).

D. RS-485 Cabling: Install at a maximum distance of 4000 feet (1220 m).

E. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from Controller to the reader is 250 feet (75 m), and install No. 20 AWG wire if maximum distance is 500 feet (150 m).
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed [250 feet (75 m)] [500 feet (150 m)] <Insert distance>.

G. Install minimum No. 18 AWG ac power wire from transformer to Controller, with a maximum distance of [25 feet (8 m)] <Insert distance>.

3.7 GROUNDING

SPEC WRITER NOTE: Revise this Article to suit Project. Coordinate with Drawings.

A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

D. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Mount on wall of main equipment room with standoff insulators.
3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.8 INSTALLATION

SPEC WRITER NOTE: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

A. System installation shall be in accordance with UL 294, manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.
B. Components shall be configured with appropriate “service points” to pinpoint system trouble in less than 30 minutes.
C. The Contractor shall install all system components including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions, documentation listed in Sections 1.4 and 1.5 of this document, and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a operable system.
D. The PACS will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or a network.
E. For integration purposes, the PACS shall be integrated where appropriate with the following associated security subsystems:
   1. CCTV:
      a. Provide 24 hour coverage of all entry points to the perimeter and agency buildings. As well as all emergency exits utilizing a fixed color camera.
      b. Be able to monitor, control and record cameras on a 24 hours basis.
      c. Be programmed automatically call up a camera when an access point is but into an alarm state.
      d. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.
   2. IDS:
      a. Be able monitor door control sensors.

b. Be able to monitor and control the IDS on a 24 hours basis.
c. Be programmed to go into an alarm state when an IDS device is put into an alarm state, and notify the operator via an audible alarm.
d. For additional PACS system requirements as they relate to the IDS, refer to Section 28 16 11, INTRUSION DETECTION SYSTEM.

3. Security Access Detection:
a. Be able to monitor all objects that have been screened with an x-ray machine and be able to monitor all data acquired by the bomb detection unit.
b. For additional PACS system requirements as they relate to the Security Access Detection, refer to Section 28 13 53, SECURITY ACCESS DETECTION.

4. EPPS:
a. Be programmed to go into an alarm state when an emergency call box or duress alarm/panic device is activated, and notify the Physical Access Control System and Database Management of an alarm event.
b. For additional PACS requirements as they relate to the EPPS, refer to Section 28 26 00, ELECTRONIC PERSONAL PROTECTION SYSTEM.

F. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

G. For programming purposes refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.

H. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system. The Contractor shall not take any corrective action without written permission from the Government.

I. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system to the Contracting Officer in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

J. Existing Equipment:

1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the design package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.
2. The Contractor shall perform a field survey, including testing and inspection of all existing door equipment and signal lines intended to be incorporated into the PACS, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include a schedule for connection to all existing equipment.
3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.
4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
5. The Contracting Officer shall be provided a full list of all equipment that is to be removed or replaced by the Contractor, to include description and serial/manufacturer numbers where possible. The Contractor shall dispose of all equipment that has been removed or replaced based upon approval of the Contracting Officer after reviewing the equipment removal list. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

K. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water and will comply with VA Master Specification 07 84 00, Firestopping. The conduit riser shall terminate

in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

L. Cold Galvanizing: All field welds and brazing on factory galvanized boxes, enclosures, and conduits shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

M. Control Panels:
   1. Connect power and signal lines to the controller.
   2. Program the panel as outlined by the design and per the manufacturer’s programming guidelines.

N. SMS:
   1. Coordinate with the VA agency’s IT personnel to place the computer on the local LAN or Intranet and provide the security system protection levels required to insure only authorized VA personnel have access to the system.
   2. Program and set-up the SMS to ensure it is in fully operation.

O. Card Readers:
   1. Connect all signal inputs and outputs as shown and specified.
   2. Terminate input signals as required.
   3. Program and address the reader as per the design package.
   4. Readers shall be surface or flushed mounted and all appropriate hardware shall be provided to ensure the unit is installed in an enclosed conduit system.

P. Biometrics:
   1. Connect all signal input and output cables along with all power cables.
   2. Program and ensure the device is in operating order.

Q. Portal Control Devices:
   1. Install all signal input and output cables as well as all power cables.
   2. Devices shall be surface or flush mounted as per the design package.
   3. Program all devices and ensure they are working.

R. Door Status Indicators:
   1. Install all signal input and output cables as well as all power cables.
   2. RTE’s shall be surface mounted and angled in a manner that they cannot be compromised from the non-secure side of a windowed door,

or allow for easy release of the locking device from a distance no greater than 6 feet from the base of the door.

3. Door position sensors shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2″ (5 cm).

S. Entry Control Devices:

1. Install all signal input and power cables.
2. Strikes and bolts shall be mounted within the door frame.
3. Mortise locks shall be mounted within the door and an electric transfer hinge shall be utilized to transfer the wire from within the door frame to the mortise lock inside the door.
4. Electromagnetic locks shall be installed with the mag-lock mounted to the door frame and the metal plate mounted to the door.

T. System Start-Up:

1. The Contractor shall not apply power to the PACS until the following items have been completed:
   a. PACS equipment items and have been set up in accordance with manufacturer's instructions.
   b. A visual inspection of the PACS has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.
   c. System wiring has been tested and verified as correctly connected as indicated.
   d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
   e. Power supplies to be connected to the PACS have been verified as the correct voltage, phasing, and frequency as indicated.
2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.
3. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Resident Engineer and Commissioning Agent. Provide a minimum of 7 days prior notice.

U. Supplemental Contractor Quality Control:

1. The Contractor shall provide the services of technical representatives who are familiar with all components and

installation procedures of the installed PACS; and are approved by the Contracting Officer.

2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

3.9 SYSTEM SOFTWARE

A. Install, configure, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.10 FIELD QUALITY CONTROL

SPEC WRITER NOTE: Retain paragraph below to require a factory-authorized service representative to perform, or assist Contractor with, field inspections, tests, and adjustments. Retain one of two options to suit Project; delete both to require only an inspection before field testing.

A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect[, test, and adjust] field-assembled components and equipment installation, including connections[, and to assist in field testing]. Report results in writing.

B. Testing Agency: [Owner will engage] [Engage] a qualified testing and inspecting agency to perform field tests and inspections and prepare test reports:

SPEC WRITER NOTE: Retain subparagraphs below with either of two paragraphs above. Edit to suit Project. Delete subparagraphs if testing will be performed by Owner-engaged testing and inspecting agency.

C. Perform the following field tests and inspections and prepare test reports:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1,

"Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.

2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

3.11 PROTECTION

A. Maintain strict security during the installation of equipment and software. Rooms housing the control station, and workstations that have been powered up shall be locked and secured, with an activated burglar alarm and access-control system reporting to a Central Station complying with UL 1610, "Central-Station Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

3.12 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.13 DEMONSTRATION AND TRAINING

A. Provide services of manufacturer’s technical representative for four hours to instruct VA personnel in operation and maintenance of units.

B. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

C. Develop separate training modules for the following:
   1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
   2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
   3. Security personnel.
   4. Hardware maintenance personnel.
   5. Corporate management.

D. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

-----END----